TIETOHALLINTO MURROKSESSA – KULUTTAJISTUMISEN VAIKUTUS ORGANISAATION ICT-YMPÄRISTÖÖN

Sami Summanen

Tampereen yliopisto
Informaatiotieteiden yksikkö
Vuorovaikutteinen teknologia
Pro gradu -tutkielma
Huhtikuu 2015

TAMPEREEN YLIOPISTO, Informaatiotieteiden yksikkö
Vuorovaikutteinen teknologia
SUMMANEN, SAMI: Tietohallinto murroksessa – kuluttajistumisen vaikutus organisaation ICT-ympäristöön
Pro gradu -tutkielma, 87 s., 2 liites.
Huhtikuu 2015

Tiivistelmä

Tässä tutkielmassa käsitellään erityisesti ICT-alaa ravistelevaa kuluttajistumisilmiötä, jossa organisaatioiden tietotekniseen ympäristöön ilmaantuu tyypillisesti edullisia, mutta alun perin kuluttajamarkkinoille suunniteltuja laitteita ja ohjelmistoja. Ilmiö on alkanut jo IBM PC:n julkistamisen jälkeen 1980-luvulla, mutta kiihtynyt merkittävästi viimeaikaisen nopean langattoman teknologian ja mobiililaitteiden kehityksen myötä.

Kuluttajateknologian työntyminen osaksi organisaatioiden IT-infrastruktuuria aiheuttaa huomattavia haasteita ja muutostarpeita tapaan, jolla tietohallinto suunnittelee, toteuttaa ja ylläpitää tietojärjestelmiä. Samalla IT-infrastruktuuriin voi tulla merkittäviä lisäpanostustarpeita. Myös organisaatioihin kohdistuvat uhkakuvat muuttuvat kuluttajistumisen muuttaessa radikaalisti tapaa, jolla työtä tehdään organisaation perinteisen tietoverkon ulkopuolella.

Tietotekniikan yleisesti hyväksyttyjen käytäntöjen mukaista on ollut jo pitkään vakioida IT-infrastruktuuri mahdollisimman pitkälle kustannushyötyjen, toiminnan tehostamisen ja ylläpitämisen helpottamisen vuoksi. Tietojärjestelmiin ja erityisesti loppukäyttäjien käyttämiin laitteisiin liittyvä kuluttajistuminen aiheuttaa merkittäviä muutospaineita tähän vakiintuneeseen käytäntöön.

Tässä tutkielmassa luodaan katsaus kuluttajistumisen historiaan ja arvioituun tulevaisuuteen sekä pohditaan sen tuomia positiivisia vaikutuksia ja ongelmia. Lisäksi esitellään mahdollisia keinoja ja teknisiä ratkaisuja, joilla ilmiölle tyypilliset sudenkuopat voidaan välttää.

Tutkielma pohjautuu kirjallisuuteen sekä kirjoittajan omiin kokemuksiin ja tehtyihin havaintoihin pitkän työuran aikana.

Tutkielmassa havaitaan, että valtaosaan kuluttajistumisilmiön tuomista haasteista löytyy jo niin teknisiä kuin hallinnollisia ratkaisuja, mutta näiden hyödyntäminen voi käydä organisaatiolle kalliiksi.

Avainsanat: kuluttajistuminen, BYOD, tietohallinto, MDM

Esipuhe

Tutkielma on tehty Tampereen yliopiston informaatiotieteiden yksikölle tammikuun 2013 ja huhtikuun 2015 välisenä aikana. Kiinnostus tätä aihetta kohtaan syntyi työelämässä kohtaamistani kuluttajistumisilmiöön liittyvistä haasteista. Ajatus tutkielman tekemisestä juuri tästä aiheesta on ollut mielessä jo vuodesta 2010.

Oman elämäni painopiste on ollut vahvasti töiden ja perhe-elämän sanelema pitkään ja vasta työpaikan vaihtaminen vuonna 2012 mahdollisti sen, että vapaa-aikaa myös opintojen loppuun saattamiselle järjestyi helpommin. Uusia tuulia tosin puhalsi jo perheen toisen lapsen syntymän myötä maaliskuussa 2013, joten lopputyön edistäminen hidastui tämän myötä tuntuvasti.

Kiitokset Jennille, Ellenille ja Danielille kaikesta tuesta ja panostuksista siihen, että sain tarvittavaa aikaa perhe-elämältä tämän työn loppuun saattamiseksi. Kiitokset työn ohjauksesta professori Roope Raisamolle ja tarkastamisesta professori Erkki Mäkiselle.

Tampereella 17.4.2015

Sami Summanen

Sisällysluettelo

1 JOHDANTO

Kuluttajistuminen (engl. *consumerization*) on terminä suhteellisen uusi, mutta viimeisen parin vuoden aikana termiä on alettu käyttämään suomalaisessakin mediassa. Nykyisin erityisesti ICT-alalla ilmiöön ei voi olla törmäämättä, ja monien organisaatioiden tietohallintoihin tämä ilmiö tuo tarvetta muutoksille niin teknologian kuin toimintatapojen osalta.

Tässä tutkielmassa kuluttajistumisella tarkoitetaan murrosta, jossa organisaatioiden teknologisen ympäristön muutosvoima tulee kuluttajarajapinnasta perinteisen isolla rahalla tuotetun ja järeän yritysinfrastruktuurin sijaan.

Tässä tutkielmassa keskitytään murrokseen, johon kuluttajistuminen voi organisaatioiden ICT-ympäristössä johtaa. Tutkielmalla pyritään selvittämään mm. kuluttajistumisen historiaa, nykytilaa ja arvioimaan tulevaisuutta sekä kartoittamaan ilmiön hyötyjä ja haittoja sekä niitä muutoksia, joita organisaatioiden ja tietohallinnon toimintaan kuluttajistumisen myötä on odotettavissa. Tutkielmassa mietitään myös kuluttajistumisen vaikutuksia ihmisten työskentelytapoihin. Koska kuluttajistumisilmiö aiheuttaa ongelmia tietoteknisen ympäristön hallinnan kanssa, tutkielmalla pyritään tarjoamaan esimerkkejä ratkaisuista, joilla ilmiön hyvät puolet saataisiin jalostettua organisaation eduksi ja haittavaikutukset minimoitua.

Lähdemateriaalina työssä on käytetty kirjallisuutta, lehti-artikkeleita, markkinatilanteen seurantaa ja Internet-aineistoa. Osa opinnäytetyön havainnoista pohjautuu omaan, usean vuoden työkokemukseen ICT:n parissa. Tavoitteenani on ollut aiheen kartoittava tutkimus.

Tutkielmani toisessa luvussa käydään läpi kuluttajistumiseen liittyvää terminologiaa, tarkastellaan ilmiön historiaa ja arvioidaan, mitä tulevaisuus tämän päivän tietämyksellä tuo tullessaan. Luvussa pyritään myös selittämään, mitä kuluttajistuminen käytännön tasolla on ja kuinka se näkyy loppukäyttäjille. Kolmannessa luvussa kartoitetaan ilmiön mahdollisia hyötyjä ja syitä sille, mikä tekee omien laitteiden käyttämisestä niin houkuttelevaa. Neljännessä ja viidennessä luvussa tarkastellaan puolestaan haasteita ja riskejä, joita kuluttajistumisen myötä voi organisaatio tai loppukäyttäjä kohdata. Näissä luvuissa pyritään myös kertomaan keinoista tai teknologioista, joilla haittavaikutuksia voi torjua tai niiden

aiheuttamia riskejä minimoida. Kuudennessa luvussa tarkastellaan organisaation tietohallinnon roolia ja haasteita tässä muuttuvassa ICT-tehtäväkentässä. Luvussa pyritään tarjoamaan ohjeita kuluttajistumisen vastaanottamiseen.

Kiinnostus aihetta kohtaan on syntynyt kirjoittajan usean vuoden työkokemuksesta erilaisten yhtiöiden tietohallinnoissa. Perinteisesti tietohallinto on vannonut jo vuosia vakioitujen toimintatapojen sekä keskitetyn ja tiukasti määritellyn IT-infrastruktuurin hallinnan nimeen, mutta viime vuosina myös Suomessa kuluttajistumisilmiön myötä tietohallinnon rooli uusien teknologioiden ja käytäntöjen suodattimena ja toimeenpanijana on muuttunut radikaalisti.

Tutkimusta kuluttajistumisen vaikutuksista on tehty viime vuosina paljon. Tutkimus kohdistuu usein yksittäisiin ilmiön seurauksiin, mutta ei niinkään vaikutuksiin organisaatioiden tietohallintojen toimintaan. Suomessa akateemista tutkimusta aiheesta ei juurikaan ole tehty, mutta muualta tutkimusta löytyy jonkin verran.

Opinnäytetyö on pyritty rajaamaan siten, että se käsittelee nimenomaan kuluttajistumisilmiötä. Vaikka opinnäytetyössä pyritään vastaamaan mm. kysymykseen, mikä on tietohallinnon rooli kuluttajistumisessa, niin tutkielmassa oletetaan lukijalla olevan perustason tietämys tietohallinnon perinteisestä roolista osana organisaation toimintaa.

Valtaosa lähdemateriaalista on haettu mm. Nelli-portaalista (National Electronic Library Interface) sekä osittain Googlen kautta. Opinnäytetyön tekemisen aikana on myös uutisvirtaa seurattu aiheeseen liittyen tiiviisti sekä mm. työtehtävien rajoissa pyritty havainnoimaan ilmiöön liittyviä seikkoja.

Tyypillisiä hakusanoja / lyhenteitä lähteiden löytämiseksi ovat olleet seuraavat:

- BYOD, CYOD, Bring Your Own Device, Choose Your Own Device
- Consumerization / Kuluttajistuminen
- Consumerization of IT / IT Consumerization
- Shadow IT / Varjo-IT
- Standardization / Standardization of IT / Vakiointi.

Koska osa lähdemateriaalista voi kadota, niin esimerkiksi ajankohtaiset aihetta sivuavat uutiset ja niiden kautta löydetyt tutkimukset on pyritty tallentamaan paikallisesti. Materiaalia kertyi opinnäytetyön aikana runsaasti, mutta niiden sisällöt olivat hyvin usein päällekkäisiä, jolloin lähdemateriaalia jouduttiin rajaamaan myös runsaasti pois.

Lähdemateriaaleista kerätyn tiedon lisäksi kirjoittajan havainnot ovat vahvasti mukana. Opinnäytetyön yksi keskeinen tavoite on ollut kirjoittajan oman näkökannan avartaminen. Artikkeleista on havaittavissa eri tahojen omat intressit ja kannat. Näin ollen artikkeleista saatavaan tietoon on pitänyt suhtautua kriittisesti.

2 KULUTTAJISTUMINEN

Tässä luvussa tarkastellaan kuluttajistumisilmiötä yleisellä tasolla. Kohdassa 2.1 tarkastellaan ilmiöön liittyvää terminologiaa ja lyhenteitä. Kohdassa 2.2 kerrotaan kuluttajistumisen historiasta sekä arvioidaan tulevaisuutta. Kohdassa 2.3 käsitellään kuluttajistumisen näkymistä käytännön tasolla. Luvun tavoitteena on tutustuttaa lukija ilmiöön liittyvään terminologiaan ja kuvata sitä, millä tavoin kuluttajistumisilmiö näyttäytyy organisaatioiden ja loppukäyttäjien arjessa.

2.1 Terminologiaa

Kuluttajistumiseen liittyy useita termejä ja niitä erilaisten artikkeleiden kirjoittajat soveltavat omia tarkoitusperiä palvellen varsin kirjavasti. Yleisimmät ilmiöön liittyvät termit ovat BYOD (Bring Your Own Device) ja CYOD (Choose Your Own Device). Erityisesti BYOD-termiä käytetään runsaasti artikkeleissa ja seminaareissa niin ulkomailla kuin meillä Suomessakin. Valtaosa organisaatioiden tietohallinnoista on tähän termiin jo tutustunut, vaikka suomenkielinen sana kuluttajistuminen olisikin vieras.

Muita ilmiöön liittyviä termejä on esitelty tarkemmin liitteessä 1. Suomenkielistä vakiintunutta terminologiaa tai akronyymikokoelmaa ei tälläkään IT-alan osa-alueella ole. Kuluttajistumisesta puhutaan yleisesti ICT-alan julkaisuissa, mutta hyvin usein niin tieteelliset aineistot kuin lehtiartikkelit käyttävät näitä englanninkielisiä akronyymejä, jotka on hyvä tunnistaa.

Yhteistä kaikille näille ilmiöön liittyville termeille on loppukäyttäjien mahdollisuus vaikuttaa teknologiavalintoihin. Ciscon Anderson [2013] kiteyttää BYOD-termin oivallisesti: “BYOD means any device, with any ownership, used anywhere.”

Kuluttajistumiseen liittyy myös hyvin läheisesti pilvipalvelut. Pilvipalvelusta puhuttaessa terminologia on niin ikään moninaista ja sitä käytetään myös markkinointipuheissa usein harhaanjohtavasti. Mellin ja Grancen [2011] mukaan pilvipalvelu on malli, jonka avulla tarjotaan kaikkialta helposti saatavissa olevaa jaettua tietojenkäsittelykapasiteettia. Ku-

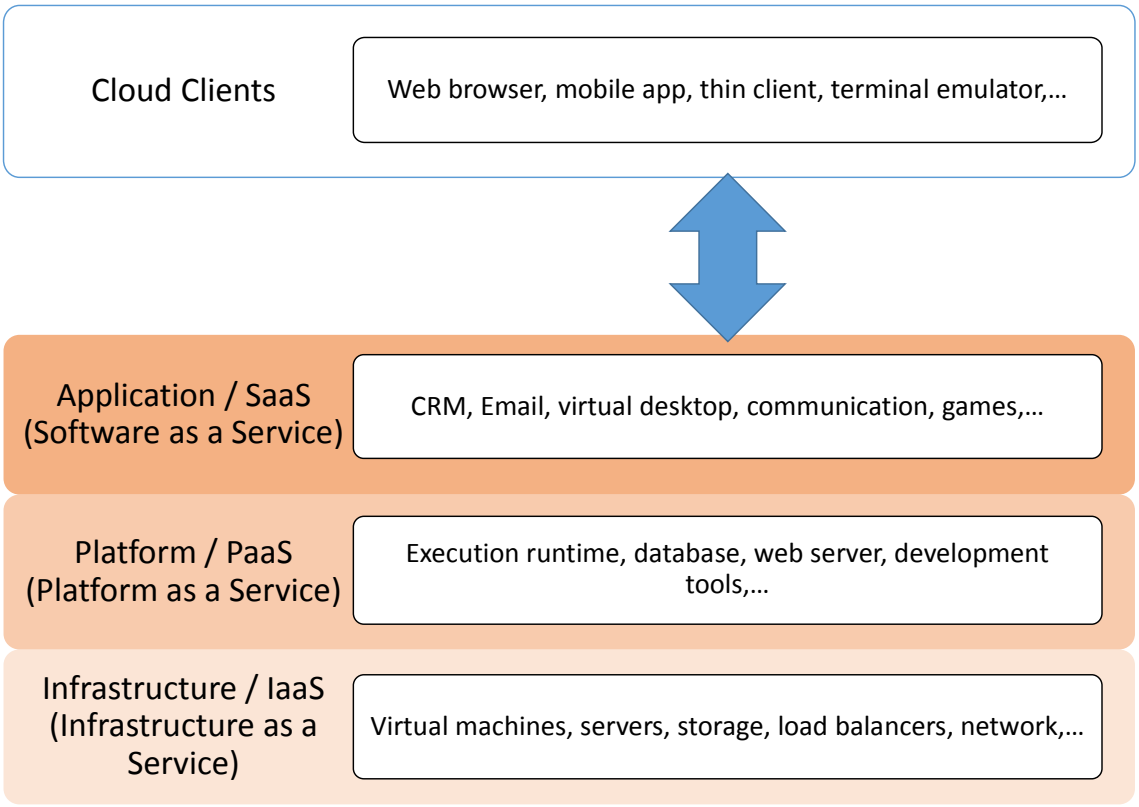
luttajistumisen kannalta olennaista tässä on mobiliteetti eikä niinkään laskentakapasiteetti. Pilvipalveluiden luonne edesauttaa vapautta päätelaitteiden valinnassa, joka on olennaista kuluttajistumisilmiölle.

Pilvipalveluja kuvaavat yleisesti seuraavat viisi ominaisuutta [Mell and Grance, 2011]:

1. Itsepalvelu: Asiakas voi omatoimisesta määritellä tarpeisiinsa sopivan määrän tietojenkäsittelyyn liittyvää kapasiteettia. Tämä on myös mahdollista automatisoida ilman vuorovaikutusta palveluntarjoajan henkilöstöön.
2. Laaja pääsy palveluun: Palvelun ominaisuudet ovat laajasti saatavilla tietoverkon kautta ja palveluun pääsee käyttämällä standardeja menetelmiä, mikä mahdollistaa palvelun käyttämisen erilaisilla laitteilla (esim. tietokoneet, tabletit, älypuhelimet).
3. Resurssien yhdistäminen: Palveluntarjoajan resursseja yhdistetään palvelemaan useita asiakkaita ja käyttäjiä. Usean vuokralaisen mallissa (multi-tenant) resurssit jaetaan dynaamisesti asiakkaan käyttöön ja resursseja voidaan säädellä kysynnän mukaan.
4. Joustavuus: Kapasiteettia voidaan lisätä ja sitä voidaan helposti myös vähentää.
5. Mitattavuus: Pilvipalvelujärjestelmät optimoivat automaattisesti resurssien käyttöä. Palvelun käyttö on mitattavissa (esim. tallennustilan käyttö, käyttäjätilien määrä ja aktiivisuus). Resurssien käyttöä voidaan seurata, valvoa ja raportoida.

Pilvipalveluilla voidaan tarkoittaa mm. seuraavia palvelumalleja (ks. kuva 1):

- IAAS – Infrastructure as a service (virtuaalikoneet, palvelimet, levyjärjestelmät, kuormantasaajat, verkot)
- PAAS – Platform as a service (tietokannat, web-palvelimet, kehitystyökalut)
- SAAS – Software as a service (sähköposti, CRM, virtuaaliset työpöydät ja sovellukset, pikaviestimet).



Kuva 1. Pilvipalveluiden jaottelu [Wikipedia, 2013]

2.2 Kuluttajistumisen historiasta ja tulevaisuudesta

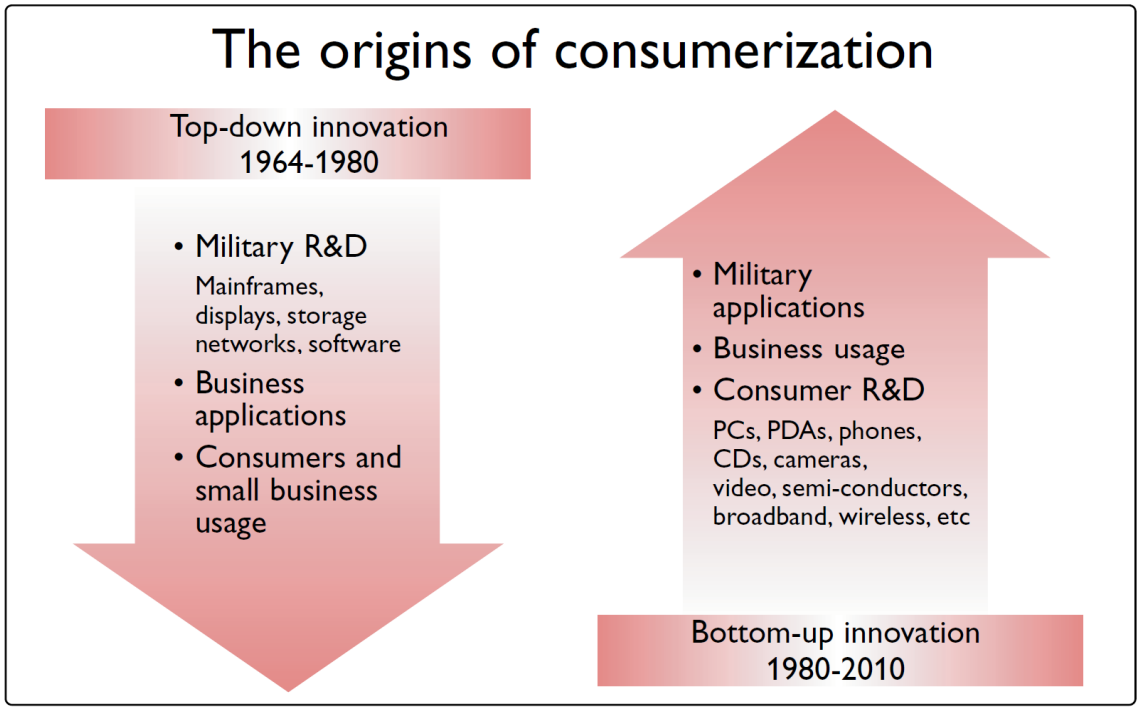
Termiä kuluttajistuminen tiettävästi alettiin käyttämään aktiivisesti ensimmäistä kertaa Leading Edge Forum -nimisessä yhtiössä vuonna 2001, mutta ensimmäisen termiä sivuavan artikkelin Leading Edge Forum julkaisi vasta vuonna 2004.

Termillä tarkoitetaan muutosta, jonka myötä uusi informaatioteknologia otetaan tyypillisesti käyttöön ensin kuluttajasovelluksissa, kuluttajien keskuudessa ja usein myös huomattavasti perinteistä organisaatiokulttuuria halvemmalla tai kuluttajan kannalta jopa näennäisen ilmaiseksi [Moschella et al., 2004]. Teknologinen innovointi tapahtuu nykyisin kuluttajateknologiassa ja muutos tekniikassa siirtyy kuluttajasovelluksista hiljalleen työpaikoille ja muihin organisaatioihin.

Muutos on yhteiskunnallisestikin todella merkittävä. Ennen 1980-lukua teknologiset innovaatiot syntyivät pitkälti suurten organisaatioiden aikaansaannoksena. Hyvänä esimerkkinä tästä on esimerkiksi Internetin kehitys [Wikipedia, 2014], joka alkoi USA:n puolustusministeriön rahoittamana ARPAnet-hankkeena, ja joka tutkimuslaitosten ja yli-

opistojen kautta alkoi laajenemaan hitaasti kohti kuluttajaa. Alkuperäinen verkon tarkoitus oli luoda vikasietoinen viestintäjärjestelmä vastaamaan Neuvostoliiton uhkaan, mutta eriydyttyään akateemiseen maailmaan ARPAnetiä alettiin kutsumaan Internetiksi. Sotateollisuuden tarpeet jaloistuivat vuosien varrella akateemisen maailman ja lopulta liikeelämän ja viihteen kulmakiveksi.

Kuvassa 2 kiteytetään kuluttajistumisilmiön juuret ja historia.



Kuva 2. Kuluttajistumisilmiön juuret [Moschella et al., 2004]

Kotikäyttöön tarkoitettujen tietokoneiden yleistymisen myötä painopiste teknologiselle innovoinnille siirtyi hitaasti kalliista keskustietokonevetoisista järjestelmistä kohti kuluttajateknologiaa. Tahti on viime vuosina kiihtynyt huomattavasti mm. älypuhelin- ja tablettikehityksen myötä. Tietojenkäsittelyn standardialusta ei enää välttämättä ole PC ja Windows, vaikka näiden osuus organisaatioiden IT-infrastruktuurista on edelleen merkittävä. Applen OS X ja Linux-distribuutiot ovat myös saaneet organisaatioissa jalansijaa ja mikäli organisaation keskeiset työkalut eivät ole käyttöjärjestelmään tiukasti sidottuja, niin valtaa teknologiavalinnassa voidaan antaa loppukäyttäjälle.

Pilvipalveluiden merkitystä ei pidä myöskään vähätellä. Tällä hetkellä uudet palvelut julkaistaan usein kuluttajille ensin ja palveluiden jalostuessa ja niiden saavuttaessa jalansijaa kuluttajamarkkinoilla niitä aletaan tuomaan myös organisaatioiden käyttöön. Hyvänä esimerkkinä tällaisesta toiminnasta on Dropbox, joka aloitti puhtaasti kuluttaja-asiakkaiden

tiedon tallennus- ja synkronointipalveluna - jopa osin ilmaisena, mutta julkaisi vuonna 2013 Dropbox for Business[1] konseptin, jolla Dropboxin käyttö saadaan organisaatioissa keskitettyyn hallintaan ja integroitumaan Active Directoryn kanssa ja mahdollistamaan kirjautumisen käyttäen organisaation keskitetysti hallinnoimia toimialuetunnuksia.

Kuluttajateknologian hinnat ovat laskeneet merkittävällä vauhdilla ja pilviteknologiaakin saa kaupan hyllyltä jo esim. Office 365[2] -paketin muodossa vaivatta. Samoja ja joidenkin mielestä myös parempia sovelluksia ja palveluita saa kuluttajapuolelta murto-osalla siitä hinnasta, mitä organisaatiot ovat tottuneet vastaavasta teknologiasta maksamaan. Muutos on saanut joissakin organisaatioissa aikaan painetta kyseenalaistaa vanhat hankintakäytännöt.

Vaikka kehitys alkoi vapaaehtoisella BYOD-mallilla, niin Gartnerin mukaan vuonna 2015 arvioidaan organisaatioiden alkavan jo edellyttämään joiltakin työntekijöiltään omien laitteiden käyttämistä. Tulevaisuudessa ei välttämättä työnantajalla ole edes tarjota tietotyövälineitä [Willis, 2013]. Tyypillisesti työntekijä saa BYOD-mallia tukevalta organisaatiolta jonkinlaisen korvauksen itse tehdyistä hankinnoista ja jos työntekijä haluaa itse panostaa rahaa työvälineisiin, joita siis voidaan joissakin tapauksissa hyödyntää myös henkilökohtaisissa tarkoituksissa, niin työntekijä saattaa joutua maksamaan loppuosuuden itse. Vuonna 2016 arvioidaan, että jopa 50 % organisaatioista sallii oman PC-laitteen hyödyntämisen työnteossa. Samalla kun tämä ilmiö yleistyy, niin työntekijöiden saamia korvauksia omien laitteiden käytöstä tultaneen laskemaan nykyisestä.

Toistaiseksi ainakin Euroopassa on kaukana tilanne, että töihin tulon edellytyksenä pidettäisiin omien laitteiden hyödyntämistä. Yksittäistapauksia kyllä löytyy. Esimerkiksi Nokian ulkoistaessa tietohallintoaan intialaiselle TATA Consultancy Services -yhtiölle tuli julkisuuteen tietoa siitä, että ulkoistetuilta työntekijöiltä edellytettäisiin omien laitteiden käyttöä [Talouselämä, 2013]. Suomessa tämä uutinen ylitti myös yleisten uutislähetysten uutiskynnyksen, sillä tällainen toimintamalli ei ole vielä Suomessa vakiintunut toisin kuin esimerkiksi Intiassa.

[1] https://www.dropbox.com/business/why-dropbox-for-business (31.1.2015)
[2] http://en.wikipedia.org/wiki/Office_365 (31.1.2015)

Accenturen vuonna 2010 tekemän maailmanlaajuisen selvityksen [Accenture, 2010] mukaan juuri kehittyvillä markkinoilla innostus omien laitteiden käyttämiseen on kiivainta. Euroopassa organisaatioiden kuluttajistumiskehitys on ollut hitainta ja siihen on suhtauduttu suurimmalla varauksella niin käyttäjien kuin organisaatioiden keskuudessa. Pohjois- ja Etelä-Amerikassa, Aasiassa ja erityisesti Intiassa kuluttajistumisen voidaan sanoa olevan jo yleistä. Intiassa, Yhdysvalloissa ja Kiinassa on myös yleistä työnhakijoiden keskuudessa, että työnantajan valinnassa yhtenä tärkeänä osatekijänä on työntekijän mahdollisuus käyttää työssään viimeisimpiä teknisiä laitteita ja ohjelmistoja. Omien laitteiden käyttömahdollisuudet ja valinnanvapaus luetaan eduksi työnantajaa valitessa. Tämä käyttäjien kaipaama työntekemisen vapaus myös vaikuttaa osaltaan etätyömahdollisuuksien lisääntymiseen ja työajan sirpaloitumiseen perinteisen työaikamallin sijaan.

Kuluttajistumistrendi tuntuu olevan kiihtymässä myös Suomessa. BYOD-ilmiöstä on Suomessa puhuttu IT-alan julkaisuissa ja tilaisuuksissa aktiivisesti nyt muutaman vuoden ajan. Suomessa nämä loppukäyttäjien teknologiavalintojen mahdollisuudet ovat lähteneet liikkeelle työpuhelimien valintamahdollisuuksien kasvulla. Enää vuoden 2008 Applen iPhonen julkistamisen jälkeen Nokian Symbian-älypuhelimet tai Blackberryt eivät välttämättä olleet niitä ainoita oikeita tietohallinnon hyväksymiä puhelimia. Organisaatioiden ruohonjuuritasolla valinnanvaraa on nykyään huomattavasti enemmän kuin vielä 5 vuotta sitten ja useissa organisaatioissa mobiililaitteiden osalta ollaan jo melko suvaitsevaisia.

Myös itsehankittujen laitteiden käyttömahdollisuudet ovat lisääntyneet. Tätä on edesauttanut mm. Mail for Exchangen / ActiveSync -protokollan laaja hyödyntäminen mobiililaitteissa [Microsoft, 2014a; Mello, 2013]. Vaikka ActiveSync ei riitä kaikkien organisaatioiden tarpeisiin, on se luonut kuitenkin perustan sille, miten kirjavaa mobiililaitekantaa voidaan perustasolla hallita. Koska merkittävä osa laite- ja ohjelmistovalmistajista maksaa ActiveSync-protokollasta lisenssimaksua, Mail for Exchange -tuki on nykyisissä älypuhelimissa erittäin kattava.

Mikä alkoi älypuhelinvalinnoilla, laajeni nopeasti vuoden 2010 Applen iPad -julkistuksen myötä myös kiinnostukseksi tabletteja kohtaan [Greengard, 2012]. Vaikka alkuun tableteille monissa piireissä naureskeltiin ja kyseenalaistettiin niiden arvo tietokoneen ja matkapuhelimen välimaastosta, nykyiset tilastot kertovat PC-myynnin hiipuneen ja tablet-

myynnin puolestaan kasvaneen merkittävästi. Useissa kotitalouksissa tabletti voikin korvata PC:n monissa tehtävissä, mutta suurempiin sisällöntuottamistarkoituksiin tabletista ei vielä ole.

Sovelluskehitystä tablet-markkinoilla on viime vuosina lisätty huomattavasti. Dropboxin, Skypen[3] ja erilaisten toimisto-ohjelmistojen kaltaisten merkittävien sovellusten tulo tableteille on lisännyt kiinnostusta tabletteja kohtaan. Runsas sovellus- ja pelitarjonta ja loppukäyttäjälle vaivaton sovellusten käyttöönotto ja intuitiivinen käyttöliittymä ovat luoneet tablet-markkinoille jo vahvan jalansijan.

Kuluttajien tablet-innostus on alkanut levitä myös organisaatioihin. Erityisesti yhtiöiden liikkuva myyntiorganisaatio ja johto kokevat tabletit tervetulleiksi. Helppokäyttöisyys ja keveys yhdistettynä pitkään akkukestoon houkuttelevat käyttäjiä. Mikäli organisaation johdossa kiinnostus tablettien käyttöön herää, niin tietohallinnon rooliksi jää usein tukea niiden käytössä ja muuttaa IT-infrastruktuuria sellaiseksi, että myös liiketoimintasovellusten käyttö tabletin avulla mahdollistuu.

Kuluttajistumisilmiön ja tablet-markkinoiden kasvamisen on arvioitu rampauttavan PC-myyntiä. Osaltaan laitteiden hankintatilastot voivat kuitenkin olla harhaanjohtavia. Esimerkiksi kotitalouksiin usein riittää yksi tietokone koko kotitalouden käyttöön, kun taas mobiililaitteet ovat usein henkilökohtaisia yhden käyttäjän laitteita ja niitä voi olla henkilön erilaisia tarpeita varten useita. Lisäksi siinä missä mobiililaitteen käyttöikä voi olla keskimäärin maksimissaan kaksi vuotta, niin PC:llä vastaava käyttöikä voi olla jopa viisi vuotta. Näin ollen uusia tietokoneita ei hankita lähellekään samalla syklillä kuin tabletteja.

PC-myynnin laskuun voi myös vaikuttaa se, että tietokoneen osto- tai uusintapäätöstä voidaan lykätä, mikäli tabletilla pystytään korvaamaan joitakin tietokoneella tehtyjä tehtäviä. Arvokkaampia tietokonelaitteita lisäksi huolletaan siinä missä edulliset rikkoutuneet mobiililaitteet helposti laitetaan kierrätykseen maksamatta huoltoa takuuajan ulkopuolella.

[3] http://www.skype.com/en/ (5.3.2015)

Lisäksi joihinkin tilastoihin voi vaikuttaa vahvasti se, että niissä ei välttämättä erotella kuluttajamarkkinoita ja organisaatioiden hankintoja toisistaan. Kuluttajamarkkinoilla on toistaiseksi enemmän kysyntää tablet-koneille, mikä osaltaan nostaa niiden markkina-osuutta huomattavasti.

Vaikka organisaatioissa PC on edelleen tavallinen näky, niin tilastot ennustavat PC-markkinoille ankeita aikoja. Gartnerin [2014] tuoreen tutkimuksen mukaan vuoden 2013 neljännellä vuosineljänneksellä PC toimitusten määrä laski 6.9 % vuoden 2012 neljännen vuosineljänneksen toimituksista. Tutkimuksen mukaan kehittyneiden maiden markkinoiden pohjakosketus PC-myynnissä on nyt kuitenkin tehty. Sen sijaan kehittyvillä markkinoilla tyypillisesti ensimmäinen verkkoon kytketty laite on usein edullinen älypuhelin ja seuraava tabletti. Tietokoneen osto saatetaan kehittyvillä markkinoilla ohittaa jopa kokonaan.

IDC:n arvioiden mukaan vuoden 2014 viimeisellä vuosineljänneksellä tablettien toimitukset ohittavat jo PC-pöytätyöasemien ja kannettavien yhteenlasketut toimitusmäärät. Arvioidaan, että vuositasolla tablettien toimitukset ohittavat PC:n toimitukset jo vuonna 2015 [Carr, 2013].

Gartnerin laskelmien mukaan [Willis, 2013] tällä hetkellä organisaatioista vain 6 % on pelkästään BYOD-kulttuurin varassa, mutta jo vuonna 2020 luku voi olla jopa 45 %. Arvion perusteella jo puolet organisaatioista edellyttäisi omien laitteiden käyttöä vuonna 2020. Vastaavasti organisaatioiden, jotka eivät hyväksy omien laitteiden käyttöä, määrä laskee vuoteen 2020 mennessä 15 % tasolle. Loput 40 % organisaatioista olisi vuonna 2020 sekaympäristöjä, joissa olisi sekä työnantajan tarjoamia laitteita että käyttäjien omia. Lopuissakin organisaatioissa, joissa työkalut annetaan organisaation puolelta, tulee pelkästään ympäristön painostuksesta johtuen käyttöön CYOD-politiikka eli tietohallinnon hyväksymien laitteiden joukosta käyttäjä saa tehdä valintansa.

Kuluttajistumisilmiö muokkaa ja ravistelee myös ohjelmistoteollisuutta. Pilvipalveluiden yleistyminen ja niiden kysyntä sekä uudet tavat käyttää useita erilaisia laitealustoja muuttaa ohjelmistoteollisuutta ja sen painopisteitä. Samalla, kun ohjelmistoja pitää tuoda pilvipalveluiden aikakauteen, niin samalla myös mm. mobiililaitteille tehtyjen sovellusten määrä tulee kasvamaan. Gartnerin [2012] arvion mukaan jo vuonna 2015 mobiilialustoille suunnattujen ohjelmistoprojektien määrä tulee olemaan nelinkertainen verrattuna

PC-ohjelmistoprojektien määrään. Tässä on toki otettava huomioon myös se, että mobiilialustalle tehtävät sovellukset voivat olla hyvinkin suppeita parin työntekijän projekteja, kun PC:lle julkaistavien ohjelmistojen koko ja kompleksisuus on tyypillisesti täysin eri tasolla.

Erityisesti mobiilisovelluksien yksinkertaisuudesta ja helposta lähestyttävyydestä johtuen käytettävyyden merkitystä BYOD-ilmiölle ei pidä vähätellä. Kuluttajat tai tässä tapauksessa työntekijät alkavat vaatia työkaluiltaan samanlaista käyttökokemusta ja helppoa lähestyttävyyttä kuin mitä kotisohvalla iPadilla on mahdollista saavuttaa. Organisaatioiden monipuoliset mutta samalla erittäin monimutkaiset ja kalliit ERP-järjestelmät, käytettävyydeltään usein hankalat tuntikirjausjärjestelmät ja monimutkaiset Groupware-ympäristöt ja sähköpostijärjestelmät eivät innosta käyttöön, jos kotona tai harrastustoiminnassa on mahdollisuus tehdä kaikki asiat vaivattomammin, tehokkaammin ja nopeammin.

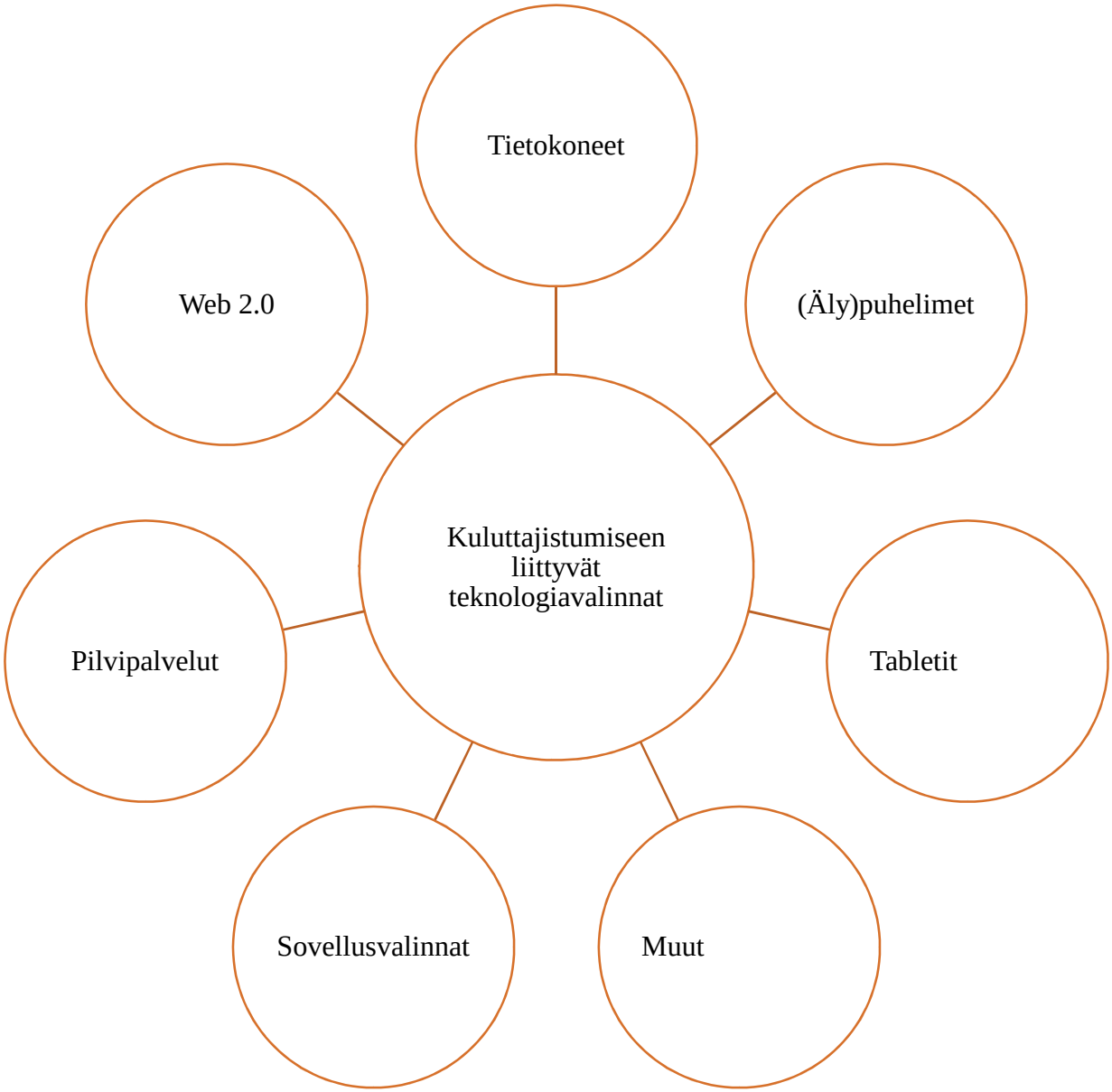
Kuluttajateknologiasta tuttua käytettävyyttä aletaan odottamaan myös työpaikalla. Jos organisaation tietohallinto ei samanlaista miellyttävää käyttökokemusta pysty tuomaan loppukäyttäjien ulottuville, niin se näkyy tyytyväisyyden laskuna IT-palveluihin ja pahimmillaan lisääntyvänä varjo-IT:nä. Vaikka käyttäjien oikeudet kutistetaan minimiin ja ohjeistuksella pyritään pitämään tietotekniikka hallinnassa, niin silti käyttäjillä on tapansa löytää kiertotiet sääntöjen ulkopuolelle ja tehdä työtä omalla tavallaan ja omilla välineillä.

Omien laitteiden hyödyntäminen on alkanut myös hiipimään oppilaitoksiin [Lacey, 2013; Sangani, 2013]. Samaa ilmiötä on hiljalleen havaittavissa Suomessakin. Omien laitteiden tullessa koululaitoksiin on herännyt keskustelua mm. tasa-arvokysymyksistä. Joillakin koululaisilla kun ei ole välttämättä varaa omien laitteiden käyttämiseen, jolloin koulun pitäisi huomioida tämä opetuksessa.

Tämä kuluttajistumisen ja digitalisoitumisen muutostahti on todella raju. Jyrki J.J. Kasvi [2014] visioi siitä, kuinka lainsäädäntö ei kansallisella ja EU-tasolla pysy tässä digitalisoitumisen kehityksessä perässä. Tulevaisuudessa uusi tekniikka 3D-tulostimista robotiikkaan ja laajennetun todellisuuden sovelluksista tulee vyörymään kuluttajamarkkinoilta työpaikoille ja koululaitoksiin tavalla tai toisella. Jos pelkkä nykyinen työasemien, tablettien, älypuhelimien ja sovellusten kirjo sekä näiden haltuunotto aiheuttaa tietohallinnoille ongelmia, niin jatkossa tilanne tulee muuttumaan yhä vain haastavammaksi.

2.3 Mitä kuluttajistuminen on käytännössä?

Kuluttajistuminen tuo ennen kaikkea työskentelyvälineisiin valinnanvapautta, jota perinteisessä raskaasti vakioidussa organisaation IT-infrastruktuurissa ei ole ollut tapana tarjota loppukäyttäjille. Kuva 3 hahmottaa joitakin valinnanmahdollisuuksia.



Kuva 3. Kuluttajistumiseen liittyviä teknologiavalintoja.

Laajasti ajatellen tekniset ratkaisut mahdollistavat aivan uudet ajasta ja paikasta riippumattomat tavat tehdä töitä.

Seuraaviin alakohtiin on avattu hieman tarkemmin näitä osa-alueita, joiden kautta ilmiö organisaatioiden arjessa näyttäytyy.

2.3.1 Tietokoneet

Nykyisin Suomessa organisaatioiden tukitoiminnot saa kuulla erityisesti uusien työntekijöiden esittämiä työasemavalintoja koskevia kysymyksiä:

- ”Saako työnteossa käyttää Applen tietokoneita?”
- ”Pääseekö kotikoneelta tekemään töitä?”
- ”Saako itse ostaa paremman koneen ja tukeeko yritys tätä hankintaa?”

Organisaatioissa edellytetään tietohallinnolta tehokkuutta, kustannussäästöjen keräämistä ja hankintojen perustelua. Tästä syystä useissa suurissa organisaatioissa työasemat ovat pitkälle vakioituja niin laitemallien osalta (muutama testattu, ylläpidetty ja tuettu valinta) kuin saatavilla olevien käyttöjärjestelmien (Windows) ja sovelluksien (Office-sovellukset yms.) osalta.

Mikäli tietohallinto kehittää automatisoidut työasemien vakiointimenetelmät tukemaan kunnolla ja asentamaan automaattisesti esimerkiksi vain Dellin tiettyjä konemalleja, niin tällöin Applen tai Lenovon koneen tuominen yhtiön verkkoon ja sen saattaminen toimintakelpoiseksi osana muuta arkkitehtuuria voi aiheuttaa tietohallinnolle ylimääräistä työtä ja tietoturvamielessä uusia tilanteita, jotka pitää huomioida.

Työasemavalinnat ja käyttäjien mieltymykset liittyvät yleensä käyttöjärjestelmään (Windows, OS X, Linux-distribuutiot). Intohimot harvemmin kohdistuvat itse laitteistoon (Lenovo, HP, Dell, Asus jne.). Poikkeuksen tähän muodostaa kuitenkin Apple, joka muodostaa erittäin merkkiuskollisen yhteisön. Sen sijaan PC-kannettavien markkinoilla erot eri laitevalmistajien välillä ovat loppukäyttäjän kannalta melko vähäisiä. Laitteissa käytetään usein samoja komponentteja ja suurin ero käytettävyyden kannalta voi tulla erilaisen näppäimistöasettelun ja kosketuslevyn / ohjaintapin toiminnasta. Erilaista käyttökokemusta kaipaavalle loppukäyttäjälle tietohallinnon onkin helpompaa perustella tietyn laitevalmistajan suosimisen PC-puolella kuin perustella, miksi loppukäyttäjän tulisi käyttää Windowsia Applen OS X:n sijaan.

Tietohallinnon kannalta sitoutuminen yhteen käyttöjärjestelmään on vakioinnin ja tukitoimintojen organisoinnin kannalta erittäin järkevää. Sen sijaan jonkun laitevalmistajan suosimista puoltavat lähinnä kustannuskysymykset.

2.3.2 Älypuhelimet

Olennainen osa kuluttajistumista on samojen laitteiden ja ohjelmistojen käyttö niin henkilökohtaisiin toimiin kuin työtehtäviin. Parhaana esimerkkinä tästä toimivat älypuhelimet, joita käytetään yleisesti sekaisin niin viihde- kuin hyötytarkoituksiin. Käyttämällä yhtä ja samaa laitetta sekä henkilökohtaisiin käyttötarkoituksiin että työnteon välineenä, loppukäyttäjät säästyvät usean laitteen käytön haasteilta. Samalla kuitenkin organisaation tietohallinnon täytyy huomioida tällaiset perinteisestä IT-järjestelmien käytöstä poikkeavat skenaariot ja rakentaa IT-infrastruktuuri tämä kaksinaiskäyttö huomioiden. Vain tämä ymmärtäen, voidaan tietoturvan taso ja käyttäjien yksityisyys varmistaa [Moschella et al., 2004; Willis, 2013].

Organisaatioiden kuluttajistumisessa juuri älypuhelimet ovat se merkittävin ja ensimmäinen teknisten laitteiden kenttä, jossa vapautumista organisaation määrittelemistä säännöistä on tapahtunut. Vielä vuosi 2012 oli varsinainen villilänsi ensimmäisillä BYOD-käyttäjillä. Vapauksia sallittiin runsaasti tietoturvallisuuden kustannuksella. Jo vuotta myöhemmin tilanne alkoi olemaan toinen, mikä näkyi mm. MDM (Mobile Device Management)[4] -tuotteiden myynnissä. Vuonna 2011 MDM-järjestelmiä myytiin 445 miljoonan dollarin edestä, kun jo vuonna 2012 niitä myytiin 790 miljoonalla. IDC arvioikin, että MDM-järjestelmien myynti kasvaa 36 % vuosittain aina vuoteen 2016 asti [Acohido, 2013].

Tällä hetkellä useissa yhtiöissä käyttäjät saavat jo kytkeä mobiililaitteitaan esimerkiksi yhtiön omaan sähköpostitiliin, mutta samalla käyttäjät joutuvat tietoturvakäytäntöjen mukaan alistumaan mm. sille, että tarvittaessa ja perustelluista syistä organisaation IT-toiminnot voivat esimerkiksi tyhjentää puhelimen etänä. BYOD-huuman alkuaikoina tällaisia rajoituksia ei vielä tunnettu, eikä niitä myöskään käyttäjien tasolla ymmärretty.

Valinnanvaraa älypuhelinvalinnoissa onkin nykyään runsain mitoin. Merkittävimmät älypuhelinvalmistajat ovat tällä hetkellä Apple (iOS) ja Samsung (Android). Lisäksi pienempiä valmistajia on, mutta valtaosa organisaatioiden älypuhelimista on nykyään Android-

[4] http://en.wikipedia.org/wiki/Mobile_device_management (31.1.2015)

tai iOS-laitteita. Suomessa myös Windows Phone -käyttöjärjestelmät ovat Nokian ansiosta melko yleisessä käytössä. Joka tapauksessa älypuhelinkenttä on huomattavasti heterogeenisempi kuin vielä 7 vuotta sitten.

Taulukossa 1 on Kantar Worldpanelin analyysi älypuhelinmyynnin markkinaosuuksista vuoden 2014 kolmelta ensimmäiseltä kuukaudelta.

Germany	3 m/e Mar 2013	3 m/e Mar 2014	% pt. Change
Android	73,6	77	3,4
BlackBerry	0,5	0,5	0
iOS	16,9	15,3	-1,6
Windows	6,1	6,6	0,5
Other	2,9	0,6	-2,3
GB	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	58,4	56,2	-2,2
BlackBerry	5,1	2,3	-2,8
iOS	28,7	32,1	3,4
Windows	7	9,1	2,1
Other	0,9	0,2	-0,7
France	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	63,3	65,1	1,8
BlackBerry	4	1,1	-2,9
iOS	21,2	23,4	2,2
Windows	7,2	8,3	1,1
Other	4,3	2	-2,3
Italy	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	62,5	70,7	8,2
BlackBerry	2,5	1,2	-1,3
iOS	19,9	12,9	-7
Windows	10,9	13,9	3
Other	4,2	1,3	-2,9
Spain	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	93,7	88,6	-5,1
BlackBerry	0,2	0	-0,2
iOS	3,1	7,6	4,5
Windows	1,3	3	1,7
Other	1,8	0,8	-1

USA	3 m/e Mar 2013	3 m/e Mar 2014	% pt. Change
Android	49,3	57,6	8,3
BlackBerry	0,9	0,7	-0,2
iOS	43,7	35,9	-7,8
Windows	5,6	5,3	-0,3
Other	0,5	0,4	-0,1
China	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	71,9	80	8,1
BlackBerry	0,3	0,1	-0,2
iOS	23,3	17,9	-5,4
Windows	1,9	1	-0,9
Other	2,6	1	-1,6
Australia	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	61,6	57,3	-4,3
BlackBerry	0,5	1	0,5
iOS	31,1	33,1	2
Windows	4,1	6,9	2,8
Other	2,7	1,7	-1
Japan	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	46	41,5	-4,5
BlackBerry	0,7	0	-0,7
iOS	49	57,6	8,6
Windows	0,3	0,9	0,6
Other	3,9	0	-3,9
EU5	**3 m/e Mar 2013**	**3 m/e Mar 2014**	**% pt. Change**
Android	69,2	70,7	1,5
BlackBerry	2,6	1,1	-1,6
iOS	19,1	19,2	0,1
Windows	6,5	8,1	1,6
Other	2,6	0,9	-1,7

Taulukko 1. Älypuhelimien markkinaosuudet – EU5 koostuu Iso-Britannian, Saksan, Ranskan, Italian ja Espanjan talousalueista [Kantar, 2014]

Kantar Worldpanelin markkina-analyysistä on luettavissa Androidin ja iOS:n selvä voittokulku niin Euroopan suurimmilla talousalueilla kuin Japanissa, Kiinassa ja USAssa. Tällaisien lukujen valossa on ymmärrettävää, miksi sovelluskehitys keskittyy Android- ja iOS-markkinoille ja Windows Phone laahaa perässä, muista alustoista puhumattakaan. Sovelluskehityspanosten myötä myös valtaosa MDM-tuotteista ja yrityssovelluksista julkaistaan ensin iOS- ja Android-alustoja tukeviksi ja mahdollisesti vasta sen jälkeen Windows Phone -laitteille.

2.3.3 Tabletit

Ensimmäisen sukupolven Apple iPad julkaistiin vuonna 2010 [Wikipedia iPad, 2014] ja täysin uudet markkinat syntyivät, vaikka kriittisimmät epäilivät tarvetta laitteelle kannettavan ja älypuhelimen välimaastosta ja pitivät Applen uutta tuotetta ylihinnoiteltuna leluna. Alkuvaiheen iPad-markkinoita auttoi varmasti iPhonen kolmessa vuodessa saavuttama jalansija ja runsas sovellustarjonta, joka suoraan toimi iPadissa – tosin ilman näyttökoolle optimoitua käyttökokemusta.

Tuote oli alun perin suunnattu kuluttajille, mutta hyvin nopeasti myös bisnesmaailma otti Apple iPadin omakseen. Erityisesti liikkuvissa työtehtävissä, joissa verkkovirtaa ei ole helposti saatavilla ja joissa kannettava olisi kömpelö käyttää, iPad on monipuolisen sovellustarjonnan, hyvän ja riittävän suuren näytön, pitkän akkukeston ja intuitiivisen kosketuskäyttöliittymän avulla myös luonut täysin uusia mahdollisuuksia työnteolle, joita aiemmin ei ole edes ajateltu [Arthur and Fox, 2011]. Applen iPadin myötä myös Android-tabletit ja Microsoftin Windows 8 -pohjaiset laitteet tulivat markkinoille ja valinnanvaraa on tänä päivänä tablet-markkinoilla jo paljon.

Sittemmin tablettien ja älypuhelimien välimaastoon on tullut ns. phablet eli tavallista suuremmalla, tyypillisesti 6-7 tuuman, näytöllä varustettu älypuhelin. Nämä ovat erityisesti Kiinan markkinoilla yleistyneet nopeasti [Kantar, 2014]. Myös älypuhelimien tuumakoot ovat kasvaneet lähemmäksi tabletteja ja nykyiset markkinoilla olevat puhelimet alkavatkin olemaan jo kooltaan sitä kokoluokkaa, ettei niitä ihan jokaiseen housuntaskuun enää saa mahtumaan. Rajat älypuhelimien ja tablettien välillä ovat alkaneet hiljalleen hämärtymään. Lisäksi markkinoille on tullut myös Asus PadFonen[5] kaltaisia hybridilaitteita, joissa älypuhelin integroituu tablet-alustaan ja toimii kuitenkin myös irrallisena älypuhelimena. Myös hybridilaitteita, joissa mukana tulee sekä Android että täysiverinen Windows-käyttöjärjestelmä, on ilmaantunut, vaikka näiden myyntivolyymit eivät kovin merkittäviä olekaan.

[5] http://en.wikipedia.org/wiki/Asus_PadFone (31.1.2015)

Työelämää ajatellen tablet vastaa käyttäjien tarpeisiin liikkuvuudesta, hyvästä akkukestosta ja pääosin hyvästä käyttökokemuksesta. Laite kulkee helposti mukana. Siinä on riittävän suuri näyttö monipuolista käyttöä ajatellen ja sovellusvalikoima kattaa nykyään jo myös yleisimmät toimistosovellukset ja kattavat pilvipalvelut, jolloin tarvittava data on aina saatavilla. Tabletit myös mahdollistavat ihan uudenlaisia käyttöskenaarioita. Esimerkiksi ilmailualalla joitakin paksuja ja usein päivittyviä manuaaleja on alettu korvaamaan tableteilla, jolloin mm. hakujen ja kirjanmerkkien tekeminen manuaalin materiaaliin on helppoa. Lisäksi tällainen laite on kokonaismassaltaan helpompi käsitellä kuin paksu paperipino. Paperisten manuaalien ylläpitäminen on vaatinut merkittävät määrät paperia ja työtä. Tämä on asia, joka tablet-aikakauteen siirtyneiden käsikirjojen osalta voidaan unohtaa ja tarvittaessa automatisoida. Lisäksi perinteiseen paperille tulostettuun manuaaliin ei ole voinut liittää esim. liikkuvaa kuvaa ja hyperlinkkejä muuhun materiaaliin, ja tämä on puolestaan sähköiselle materiaalille mahdollista ja jopa suotavaa.

Työelämässä erityisesti asiakasrajapinnassa työskentelevät myyntimiehet ja johtajat ovat mielellään ottaneet tabletit omakseen. Tyypillisen tabletin akkukeston ja keveyden ansiosta laitetta voi käyttää ilman verkkovirtaa pidemmänkin työpäivän ajan ja laaja sovellusvalikoima ja kattavat verkko-ominaisuudet huolehtivat siitä, että osa työstä tai joissakin tapauksissa jopa kaikki työn osa-alueet hoituvat ilman varsinaista tietokonetta työmatkan aikana. Myös esimerkiksi tuoteportfolioiden esittelyt tabletin näytöltä ovat näytön koko huomioiden kätevää.

Tableteista (tai älypuhelimista) voi olla myös hyötyä esimerkiksi logistiikkatehtävissä. Varastotyöntekijälle digikameralla varustettu helppokäyttöinen ja akkukestoltaan riittävä kosketusnäyttölaite voi olla omiaan helpottamaan esim. viivakoodien lukemista ja erilaisia varastotyössä tarvittaviin tietokantoihin pääsyä.

Oivallinen esimerkki tablettien vaikutuksesta perinteisiin markkinoihin voidaan havaita kassalaitteiden kehityksessä. Suomessakin esimerkiksi Nettitieto Oy tarjoaa melko edulliseen hintaan Mobiilikassa[6]-nimistä iPad-sovellusta, jolla voi korvata perinteisen kassakoneen. Sovellus yhdessä iPadin kanssa palvelee erityisen hyvin kauppiaita, jotka tekevät

[6] http://www.mobiilikassa.fi/ (31.1.2015)

liikkuvaa myyntityötä tai messumyyntiä. Yleensä kassajärjestelmä on ollut raskas ja tilaa vievä sekä arvokas ostaa ja ylläpitää, mutta pienyrityksen tarpeisiin tällaiset iPad-sovellukset voivat tarjota edullisen tavan hallita kassatapahtumia, tulostaa raportteja kirjanpitoa varten ja huolehtia ylläpidosta itse ilman erillisiä ylläpitosopimuksia kassajärjestelmän tarjoajan suuntaan. Tabletin varaan rakennetut kevyet kassajärjestelmät voivat kilpailutilannetta ravistellessa samalla vaikuttaa positiivisesti perinteisten kaupan alan järjestelmien kehitystyöhön.

Tässä mainitut esimerkit tablettien käyttökohteista työelämässä ovat hyvin rajattuja. Sovellusvalikoima on jo niin valtava, että merkittävä osa sellaisista tehtävistä, joissa sisällöntuottaminen näppäimistön avulla ei ole tarpeellista, hoituu jo tablettien avulla. Näin ollen on ymmärrettävää, miksi tablettien käyttöönotoista yritysmaailmassa puhutaan paljon ja miksi myös tavalliset työntekijät voivat kysyä mahdollisuuksista hyödyntää omia tablet-laitteita firman tietoteknisiin resursseihin pääsemisessä.

2.3.4 Sovellusvalinnat

Edellä mainitut kuluttajistumiseen liittyvät osa-alueet ovat liittyneet laitteisiin, mutta vähintään yhtä merkittävässä roolissa kuluttajistumisessa ovat sovellusohjelmistoihin liittyvät valinnat. Tyypillisessä organisaatiossa sovellusvalikoima pyritään pitämään vakioituna ja mielellään suppeana mm. sovellusten jakelun, ylläpidon ja lisenssihallinnan helpottamiseksi.

Normaalikäyttöä ajatellen organisaation tietokoneilta löytyy usein tavalliset toimisto-ohjelmat (esim. Microsoft Office), PDF-lukijat (esim. Adobe Reader), verkkoselaimet, sähköpostiohjelmat, pikaviestimet, tietoturvaohjelmistot ja peruskäyttöä tukevat apuohjelmistot kuten pakattujen tiedostojen käsittelyyn liittyvät ohjelmat. Näiden perusohjelmien lisäksi mm. liiketoimintakohtaiset sovellusohjelmat ovat keskeisessä roolissa.

Aivan kuten laitteiden valinnoissa, kuluttajistumistrendi aiheuttaa painetta myös sovellusvalintoihin liittyen. Organisaatiossa esim. kuvankäsittely voi joltakin henkilöltä sujua luontevimmin Adobe Photoshopilla ja toinen voi päästä hyviin tuloksiin esim. GIMP:n kaltaisilla ilmaisohjelmistoilla. Kotona tai vanhoissa työympäristöissä opitut ohjelmat ovat usein niitä, joita jatkossakin käyttäjä toivoisi voivansa käyttää.

Joissain yhteyksissä tätä sovellusvalintoihin liittyvää kuluttajistumiskenttää kutsutaan termillä BYOA (Bring Your Own Application) [McIlwain, 2011].

2.3.5 Pilvipalvelut ja Web 2.0

Osittain sovellusvalintoihin liittyen pilvipalvelut ovat niin hyvässä kuin pahassa osa tätä kuluttajistumisen trendiä. Useat pilvipalvelut ovat saavuttaneet jalansijansa ensin kuluttajamarkkinoilla ja vasta miljoonien käyttäjien myötä tuotetta on alettu markkinoimaan organisaatioiden käytettäväksi.

Useisiin organisaatioihin pilvipalvelut ovat hiipineet takaoven kautta jo kauan ennen kuin pilvipalvelua on tuotteistettua organisaation tarpeita ajatellen. Esim. Google Driven[7] ja Microsoftin OneDriven[8] kannalta Google Gmail / Outlook -postin käyttäjät saavat saman www-selainkäyttöliittymän kautta käyttöönsä pilvitallennuspalvelut. Hyvin usein organisaatioissa jopa ohjeistetaan käyttäjiä hoitamaan henkilökohtaiset asiansa oman sähköpostitilinsä kautta. Näin ollen em. palvelut ovat usein auki organisaation verkosta, jolloin myös pilvitallennuspalveluihin on verkkosivun käyttöliittymän kautta vapaa pääsy. Tällaisien pilvitallennuspalveluiden avulla työntekijä on pystynyt liikuttamaan organisaation dataa kotiinsa ja mobiililaitteisiin hyvin pienellä vaivalla, jotta työntekoa on pystynyt jatkamaan kotioloissa – on siihen lupa tai ei. Samalla on voinut liikkua toisaalta henkilökohtaista tietosisältöä organisaation verkon suuntaan.

Suuria pilvitallennuspalveluita ovat mm. Dropbox, Google Drive ja Microsoft OneDrive. Lisäksi pilvipalveluina saa paljon muutakin loppukäyttäjää kiinnostavaa. Tarjolla on mm. viestintään liittyviä palveluita, toimisto-ohjelmistojen ja tiimityön välineitä (esim. Microsoft Office Online[9] ja Google Apps for Work[10]), muistiinpanosovelluksia kuten Evernote[11], varmuuskopiointiin erikoistuneita palveluita kuten CrashPlan[12], BackBlaze[13] ja

[7] https://www.google.com/drive/ (31.1.2015)
[8] https://onedrive.live.com/about/en-us/ (31.1.2015)
[9] http://products.office.com/en-us/office-online/documents-spreadsheets-presentations-office-online (31.1.2015)
[10] https://www.google.com/work/apps/business/products.html (31.1.2015)
[11] https://evernote.com/ (31.1.2015)
[12] http://www.code42.com/crashplan/ (31.1.2015)
[13] https://www.backblaze.com/ (31.1.2015)

Carbonite[14] sekä salasanataakkaa helpottamaan luotuja pilvipohjaisia ratkaisuita kuten Lastpass[15].

Yhteistä edellä mainituille pilvipalveluille on verkkoon pilvipalveluun tapahtuvat tallennukset ja useissa palveluissa myös laaja päätelaitetuki ja älypuhelinmalleihin kehitetyt erilliset sovellukset. Valtaosaa näitä pilvipalveluita vaivaa sellaisenaan hallinnan puute organisaatioita ajatellen. Tällaiset pilvipalvelusovellukset ajautuvat helposti varjo-IT:n puolelle, koska käyttäjille niiden hankinta ja käyttö on äärimmäisen vaivatonta ja esim. tietohallintoa ei välttämättä haluta edes informoida kaikista työntekoa helpottamaan tehdyistä ratkaisuista, koska pelkona voi olla näiden eksplisiittinen kieltäminen ja tekninen estäminen.

Edellä mainittujen konkreettisten esimerkkien lisäksi voidaan ajatella laajemmin, että sosiaalisen median ja Web 2.0:n myötä erilaisten vuorovaikutteisten Wikien ja blogien kuluttajistuminen ja käyttäjäkeskeiset palvelut ovat myös hiipineet organisaatioiden tietotekniseen ympäristöön sisälle [O'Reilly, 2005]. Nämäkin tyypillisesti ovat lähtöisin kuluttajapuolelta, mutta jalostuneet myöhemmin organisaatioiden tarpeisiin. Esimerkkinä tällaisesta jalostuksesta voisi pitää Microsoftin Yammer-palvelua[16], jota voidaan pitää organisaatiokäyttöön tarkoitettuna Facebook-palveluna.

Monipuolisien pilvipohjaisten sovellusten lisäksi pilvestä saa ostettua myös IT-infraa ajatellen esimerkiksi palvelinkapasiteettia, mutta käytännön tasolla tämä ei välttämättä erotu loppukäyttäjälle millään tavallisesta organisaation omasta konehuoneesta tulevasta palvelusta. Suurin ero pilvestä ostetun ja oman konehuoneen ratkaisun erona voidaan pitää skaalautuvuutta ja ketteryyttä, jolla pilvestä uutta kapasiteettia saa hankittua ja toisaalta poistettua.

[14] http://www.carbonite.com/ (31.1.2015)
[15] https://lastpass.com/ (31.1.2015)
[16] http://en.wikipedia.org/wiki/Yammer (31.1.2015)

2.3.6 Paikka ja aika

Yksi olennaisimmista syistä kasvavalle kuluttajistumistrendille on mobiliteetin kasvu langattomien verkkojen ja mobiililaitteiden kehityttyä nykytilaansa. Kuluttajat ovat jo tottuneet siihen, että esimerkiksi pankkiasioiden ja yhteydenpidon hoitaminen ei edellytä enää kiinteää puhelinlinjaa, työpistettä ja pöytätietokonetta. Kun pankkiyhteydetkin hoituvat kätevästi julkisilla kulkuvälineillä liikkuessa, niin sitä samaa joustavuutta on alettu odottamaan työnantajalta ja työnantajan tarjoamilta työskentelyvälineiltä.

Työn tuloksen kannalta ei enää vuonna 2020 välttämättä ole olennaista leimata itsensä työpaikalle sisään kello 8.00 ja ulos kello 16.00. Tulevaisuudessa työsuorituksia ja tuottavuutta saatetaan mitata aivan eri tavoilla kuin kellokortilla. Työpaikalla oleminen ei ole sama asia kuin tuottavan työn tekeminen. Tämä osaltaan mullistaa myös esim. työsuojeluun liittyviä säännöksiä, jotka eivät ole pysyneet teknisen kehityksen vauhdissa mukana.

Nykyiset palvelut alkavat jo mahdollistamaan todella joustavat tavat tehdä töitä. Sähköposti ja käytännössä kaikki viestintä kulkee helposti mukana myös älypuhelimessa. Joitakin liiketoimintasovelluksiakin saattaa pystyä käyttämään mukana kulkevalla laitteella. Pilvipalveluista tuotetut sähköposti-, intranet-, pikaviesti- ja tiedostopalvelut ovat pääsääntöisesti helpommin saatavilla olevia kuin organisaation omassa konehuoneessa pyörivät palvelut. Nämä kaikki mahdollistavat huomattavasti joustavammat toimintatavat kun työssä aloitetun tehtävän jatkaminen kotona inspiraation sanelemana on ainakin teknisestä näkökulmasta mahdollista ja jopa helppoa – vaikka se ei välttämättä tietoturvaorganisaatiota, palkanlaskentaa ja työsuojeluviranomaisia miellyttäisi.

Varsinkin luovalla alalla, jossa esimerkiksi ohjelmoija tai yliopiston tutkija saattaa saada sen parhaan inspiraation jossain aivan muualla kuin työpaikalla, päätelaitevapaus ja pääsy tarvittaviin digitaalisiin organisaation palveluihin helposti ilman valtavia ponnisteluja on niin organisaation kuin yksilön etu. Parhaat työhön liittyvät innovaatiot saattavat syntyä todella poikkeuksellisissa olosuhteissa.

Kolikolla on kuitenkin kääntöpuolensa. Tämä rajojen hämärtyminen voi aiheuttaa pahimmillaan levottomuutta, kun kotona ei enää saa viettää aitoa vapaa-aikaa. Joissakin organisaatioissa ongelmaa voidaan hallita esim. määrittelemällä kellonaikarajat tunnuksien kirjautumisille tietojärjestelmiin tai asettamalle esimerkiksi mobiililaitteille aikarajat, jol-

loin sähköpostin synkronointi toimii automaattisesti. Tämä on asia, jonka kanssa kannattaa olla varuillaan, koska tunnolliset työntekijät voivat polttaa itsensä helposti loppuun [Savvas, 2012].

2.3.7 Yhteiskunnan digitalisoituminen

Tämä koko BYOD-ilmiö on pieni osa sitä suurempaa työelämän mullistusta ja yhteiskunnan digitalisoitumista [Kasvi, 2014], jossa raja-aidat työpaikan ja työajan sekä kodin ja vapaa-ajan väliltä hämärtyvät. Seurauksena tulee olemaan myös nykyisten yhteiskunnallisten rakenteiden uudelleenjärjestelyä, kun uusi teknologia syrjäyttää joitakin toimenkuvia ja toimialoja täysin ja muuttaa esimerkiksi kaupan alaa pysyvästi. Kaikessa tässä kehityksessä niin lainsäätäjien kuin organisaatiotasolla hallintoon liittyvien yksiköiden tulee olla hereillä. Muutosvauhti on kiihtyvä ja organisaatiot, jotka pyrkivät välttämään ilmiön haltuunottoa ja muutosjohtamista, tulevat ajautumaan helposti kilpailukyvyn menetykseen.

Kiihtyvän digitalisoitumisen myötä BYOD-ilmiö ei tule rajoittumaan lopulta pelkkään työasemien, tablettien, älypuhelimien ja näiden sovelluksien valintakysymyksiin, vaan tekniikan kehittyessä organisaatioiden on otettava kantaa myös esimerkiksi Google Glassin[17] tai Microsoft HoloLensin[18] kaltaisiin täysin uudenlaisiin laitteisiin ja sovelluksiin.

Jos organisaatioiden hallinnolla on hankalaa, niin lainsäädäntöelimillä on vielä vaikeampaa pysyä kehityksessä mukana [Kasvi, 2014]. Jotta yhteiskunnan digitalisoituessa mahdollistettaisiin yritysten kasvumahdollisuudet uudessa markkinatilanteessa, tulisi lainsäädäntöelimien olla kehityksessä mukana eikä seurata vuosikymmen perässä.

Paljon on esimerkkejä siitä, kuinka myös Suomessa innovatiiviset uudet verkkopalvelut ammutaan alas viranomaisten tai tekijänoikeusjärjestöjen vuoksi. Esimerkkeinä voidaan mainita mm. Bookabooka-palvelu[19], jonka tarkoitus oli tarjota opiskelijoille kurssikirjavuokrausta. Tekijänoikeusjärjestöt laittoivat toiminnalle käytännössä pisteen, kun samaan

[17] http://en.wikipedia.org/wiki/Google_Glass (5.3.2015)
[18] http://www.microsoft.com/microsoft-hololens/en-us (5.3.2015)
[19] http://www.bookabooka.fi/ (31.1.2015)

aikaan Chegg.com[20] lähti vastaaville markkinoille Yhdysvalloista. Chegg.com:n liikevaihto on sadoissa miljoonissa ja on vain ajan kysymys, milloin ko. palvelu valloittaa myös Suomen markkinoita [Kasvi, 2014]. Suomessa vanhoja reviireitä pyritään tyypillisesti puolustamaan. Tässä on selvä ero esimerkiksi tilanteeseen Yhdysvalloissa. Jos uusi palvelu tuo mukanaan jotain aivan uutta ja innovatiivista, niin Suomessa ja EU:ssa on helposti enemmän jarrutusta edessä lakien, asetusten ja erilaisten omia etujaan ajavien järjestöjen muodossa. Yhdysvaltojen puolella yleensä asiat pystytään sopimaan – rahalla, jos ei muuten. Luultavasti osittain tästä syystä EU:n puolelta ei ole merkittäviä verkkopalveluita tarjolla, vaan suurimmat ja nimekkäimmät on perustettu USA:n joustavampien käytäntöjen puolella. Tästä kuitenkin poikkeuksena voidaan mainita Skype, joka sai alkunsa Virosta.

Tämä vastaava reviiriajattelu liittyy myös kuluttajistumisilmiöön. Muutosvastarinta on melkoinen, kun asioita pyritään tekemään uudella tavalla. Tämä heijastuu myös siihen, että mm. Yhdysvalloissa BYOD-kulttuuri on omaksuttu aivan eri tavalla käyttöön kuin Euroopassa. Tietohallinnot ottavat helposti puolustuskannan, jos totutut käytännöt ja rutiinit tulevat uhatuksi. Tukitoiminnoissa työskenteleviä voi arveluttaa tilanne, jossa esimerkiksi työasemien asennus ja tukitoimia pyritään vierittämään käyttäjien varaan – tällöin tiettyjen tukifunktioiden työpaikat voivat olla vähentämisuhan alla. Tämä ei kuitenkaan suoraan välttämättä vähennä tietohallinnon työtä, mutta työnkuva saattaa muuttua syvällisempää ja monipuolisempaa osaamista vaativaksi ja mm. arkkitehtien sekä sovellusintegraatioista vastaavien työtehtävien määrä ja haastavuus voivat kasvaa uusia järjestelmiä ja toimintamalleja käyttöönotettaessa.

[20] http://www.chegg.com/ (31.1.2015)

3 KULUTTAJISTUMISEN HYÖTYNÄKÖKULMAT

Tässä luvussa pyritään selvittämään, mitä hyötyjä kuluttajistumisesta on organisaation ja yksilön näkökulmasta. Kappaleen tavoitteena on myös selvittää syitä viimeaikaiselle BYOD-innostukselle. Kohdassa 3.1 pohditaan yleisellä tasolla kuluttajistumisesta tulevia keskeisiä hyötyjä ja kohdassa 3.2 nostetaan esille Ciscon BYOD-toteutus omassa ICT-ympäristössään.

3.1 Kuluttajistumisen hyödyistä

Kuluttajistumista markkinoidaan usein mm. kustannussäästöillä, työn tehostamisella ja työntekijöiden motivaation parantamisella. Seuraavissa alakohdissa tarkastellaan tyypillisiä kuluttajistumiseen liittyviä hyötynäkökulmia – kustannustekijöitä, tehokkuutta, vaikutuksia työmotivaatioon ja tuottavuuteen.

3.1.1 Kustannustekijät

Keskeisenä kuluttajistumistrendin vauhdittajana on pidetty kustannustekijöitä. Kuluttajateknologia on yritysmaailman vastaavaan verrattuna pääosin edullisempaa. Tavallisesta marketista voi saada teknisiltä ominaisuuksilta ylivertaisen laitteen euromäärällisesti huomattavasti edullisemmin kuin suosimalla organisaatioiden usein hyvin konservatiivisia ja tylsiä valintoja. Pienistä hankintapuroista voi syntyä iso virta. Jos 100-200 euron säästö työasemaa (laitteisto + käyttöjärjestelmä) kohden kerrotaan esimerkiksi tuhannella uusittavalla työasemalla vuotta kohden, niin puhutaan jo hankintakuluissa satojentuhansien eurojen toistuvasta, vuosittaisesta, säästöstä.

Tietohallintopäättäjien BYOD-innostusta ruokkivat myös helposti tutkimukset, joiden mukaan jotkut käyttäjät ovat jopa halukkaita sijoittamaan omaa rahaa laitteisiin tai esimerkiksi internet-liittymiin, joita sitten voidaan hyödyntää myös töiden tekemiseen. Usein käyttäjillä motivaationlähteenä näihin sijoituksiin ovat omat mieltymykset ja totutut käytännöt tietoteknisten asioiden hoidossa.

Kustannustekijöihin tulee kuitenkin suhtautua monestakin syystä varauksellisesti. Pitkään ICT-ala on vannonut esimerkiksi työasemien vakioinnin nimeen keskitetyn hallinnan, hallinnointityön selkeyden ja kustannustehokkuuden vuoksi [Peters, 2008]. Mitä kirjavammaksi organisaatioiden laite- ja sovelluskanta muodostuu sitä kovempi työ tietohallinnolla ja tukiorganisaatiolla on laitteiden ja sovellusten tukemisessa sekä vakiointijärjestelmien kehittämisessä, ylläpidossa ja hallinnoinnissa.

Vakioinnissa voi olla monta tasoa. Peters [2008] jakaa vakiointikohteet viiteen luokkaan:

1) laitteet,
2) käyttöjärjestelmät,
3) ohjelmistot,
4) kauppiaat / tukkurit, ja
5) sekalaiset hankinnat.

Perinteisesti tietohallinto on varsinkin suurissa organisaatioissa pyrkinyt vakioimaan em. listalta suurimman osan – samalla ottaen vastuulleen IT-tarvikkeiden hankintavastuun.

Vakioimalla esimerkiksi laitteet muutamaan tuettuun saman laitevalmistajan laitteeseen ja työasemien käyttöjärjestelmät esimerkiksi Windows 7 64-bittiseen versioon, on voitu laitteistojen ja sovellusten yhteensopivuusongelmia merkittävästi vähentää sekä helpottaa tukitoimintojen kuormitusta, kun erilaiset laitekombinaatiot käyvät helpommin tukihenkilöille tutuksi. Vakioimalla kerrallaan käytössä olevat työasemakäyttöjärjestelmät ei ole pelkästään pystytty vähentämään tukipalveluiden haasteita, loppukäyttäjien ohjeistuksia ja koulutuksia, mutta myös pitämään huolta siitä, että sovelluspuoli voi pysyä hallittavissa mitoissa, kun tietohallinnon ei tarvitse varmistaa sovellusten toimivuutta useilla eri käyttöjärjestelmäversioilla. Tietohallinnon toimintojen kannalta pahinta on se, että tukea joutuu antamaan yhtaikaa esimerkiksi 32-bittiselle Windows XP:lle ja 64-bittiselle Windows 7:lle. Tällainen usean käyttöjärjestelmäversion yhtaikainen tukeminen kasvattaa helposti ympäristön kompleksisuutta, lisää yhteensopivuusongelmia ja voi aiheuttaa myös uusia sovellushankintoja vanhojen rinnalle, joita niitäkin saattaa joutua edelleen käyttämään.

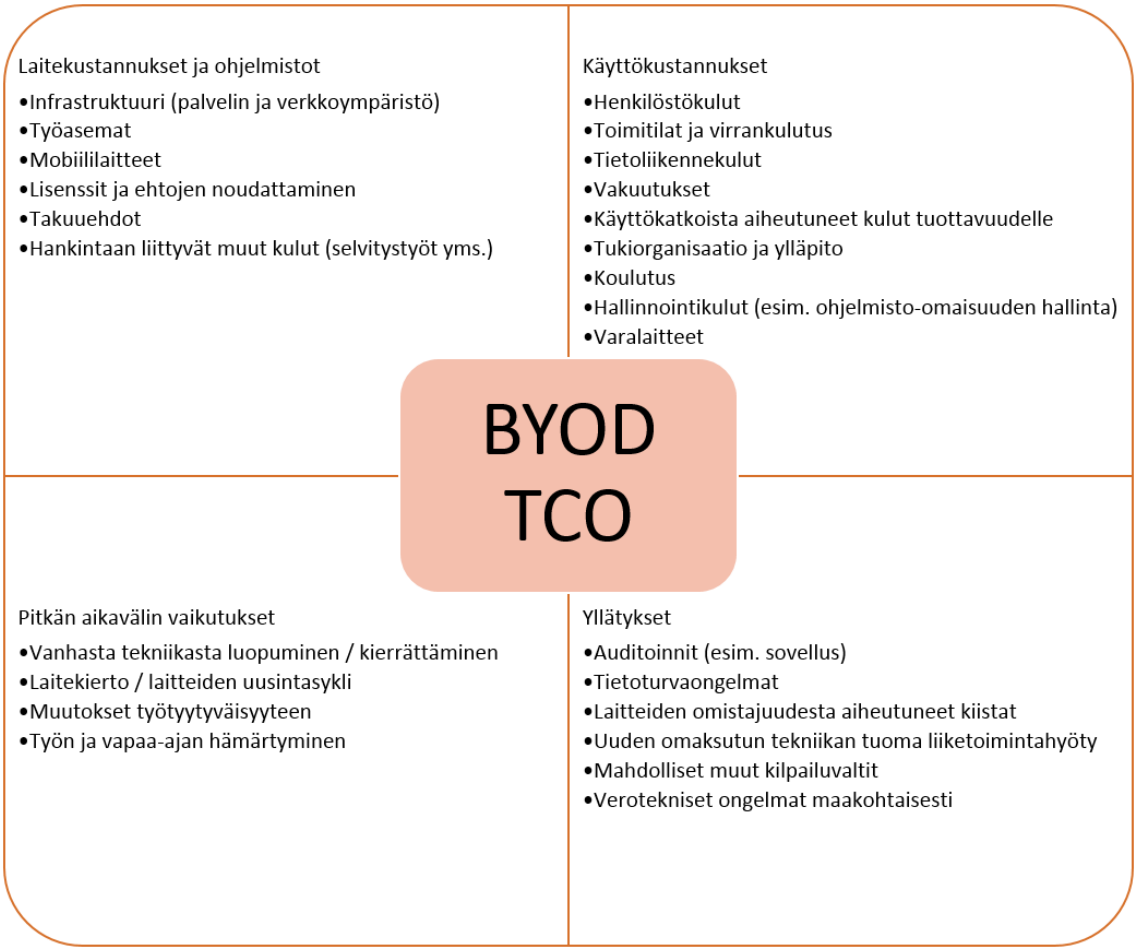
Hankintoja keskittämällä esim. yhdelle tukkurille helpottuu hallinnollinen työ huomattavasti, vaikka tällöin voi joutua joistakin tuotteista maksamaan enemmän kuin kilpailijalta. Useat laitevalmistajat myöntävät volyymialennuksia, kun tilausten yhteenlaskettu määrä ylittää tietyt kriteerit. Volyymialennuksilla voi listahinnoista tippua parhaimmillaan jopa

50 %, jolloin esim. PC-yrityskoneiden hinta alkaa olemaan samassa luokassa kuluttajille suunnattujen laitteiden kanssa. Samalla keskittämisellä saavutetaan myös hyötyjä mm. huoltojen järjestämisessä, koska useilla valmistajilla on toisistaan rajusti eroavia huoltokäytäntöjä.

Vakiointitasoja voi BYOD-aikakaudella olla kuitenkin useita ja joustaminen on mahdollista. Mikäli organisaatiossa esim. vakioidaan ainoastaan sovellusten hyväksyntä prosessit ja sovellusjakelu, mutta edellytetään omien laitteiden käyttäjiltä oman laitteen hankintaa, asentamista ja konfigurointia organisaation infrastruktuurikelpoiseksi, niin IT-tukitoimintojen kuormitus jää alhaisemmaksi. Jos käyttäjän vastuulle asetetaan myös laitteen elinkaaren huoltosopimuksista huolehtiminen, niin tukitoimintojen kuormitus laskee entisestään.

Omien laitteiden käytöstä aiheutuvat kokonaiskustannukset (TCO, Total Cost of Ownership) on kuitenkin erityisen vaikea laskea ennakoiden BYOD / CYOD -politiikkaa ajatellen. Todelliset kustannukset selviävät helpommin vasta vuosien kuluttua BYOD-mallin käyttöönoton jälkeen ja nämäkin ainoastaan siinä tapauksessa, että organisaatiossa on riittävästi mittareita, joita vertailemalla voi omien laitteiden käytöstä aiheutuvien kustannusten kokonaisvaikutusta arvioida. Toimialakohtaiset erot ovat suuria. TCO-laskentaan vaikuttaa suuresti organisaation ikä, toimiala, organisaation kulttuuri ja yleinen teknisen osaamisen taso työntekijöiden keskuudessa.

Kuvaan 4 on hahmoteltu joitakin asioita, jotka pitäisi ottaa huomioon arvioitaessa BYOD-politiikan käyttöönottoa ja siitä saatavia hyötyjä.



Kuva 4. BYOD-politiikkaan liittyvää kustannuskenttää

Hankintakustannusten sälyttäminen loppukäyttäjälle yleensä laskee organisaation suoria kuluja, mutta yllätyksiä kulujen suhteen voi olla luvassa esim. lisääntyvän mobiilidatan käytön myötä. Tyypillinen ongelma on myös lisääntyvän IT-tuen kustannukset. Kustannussäästöjä voi syntyä, mikäli tietohallinnon ja loppukäyttäjien vastuualueet ovat selvillä ja muutos pidetään hallittuna [Rangaswami, 2012]. Tietohallinto voi esimerkiksi vakioida sovelluspuolta ja loppukäyttäjä huolehtii omasta laitteestaan alkaen huoltosopimuksen toimivuudesta, huoltojen tilaamiseen ja järjestämiseen, käyttöjärjestelmän asentamiseen ja peruskonfigurointiin. Järkevintä on muutoshallinnan kannalta tehdä BYOD-politiikasta kristallinkirkas niin tietohallinnolle kuin loppukäyttäjälle ja tehdä tarkat raamit sille minkälaiset laitteet ovat sallittuja sekä minkälaisia ehtoja laitteiden ja niiden huoltosopimusten pitää täyttää. Lisäksi pitää olla selvitetty ja ohjeistettu tarkoin, miten omien laitteiden kytkeminen organisaation tietojärjestelmiin tapahtuu. Ohjeistuksen pitää myös seurata aikaansa ja se pitäisi tarkistaa esimerkiksi puolivuosittain, koska teknologinen kehitys on niin nopeaa. Vuonna 2010 laadittu BYOD-ohjesäännöstö ei ole enää muutamaa vuotta myöhemmin sellaisenaan kelvollinen.

Ecarin tekemän tutkimuksen mukaan [Dahlstrom and diFilipo, 2013; Dahlstrom, 2013] BYOD-mallin käyttöönotosta syntyvät kustannussäästöt eivät ole itsestäänselvyys. Paljon riippuu organisaation nykyisen tietoteknisen infrastruktuurin tilasta. Infran päivittämiseen sijoitettu raha voi olla huomattavasti BYOD-ilmiöstä saatuja suoria kustannushyötyjä suurempi. Jos infrastruktuuri ja organisaation prosessit ovat omien laitteiden käyttöönoton kannalta valmiita, niin kustannussäästöjä voi syntyä. Yleensä kuitenkin infraa ajatellen joitakin uusia hankintoja joudutaan tekemään, jotta omien laitteiden käyttö mahdollistuu hallitusti.

Samankaltaisiin tuloksiin on päätynyt mm. Harris ja muut [2012] kyselytutkimuksessaan. BYOD-käytäntöjen myötä suoria säästöjä esim. laitehankinnoista voi tulla, mutta ympäristön ja hallinnoinnin monimutkaistuessa säästöistä ei käytännössä voida enää puhua.

Joitakin kustannushyötyjä voidaan myös löytää hallinnolliselta puolelta, kuten Airwatch [2012] asian ilmaisee. Työntekijälle voidaan jopa luovuttaa esimerkiksi tietoliikenne ja puhelinliittymiin liittyvä hallinnollinen työ, jolloin työntekijä saa vapaat kädet huolehtia siitä, että liittymä vastaa tarpeita, mutta toisaalta työntekijän vastuulle siirtyy kaikki hallinnointi – joissakin tapauksissa myös laskujen maksaminen ja tämä kaikki voi olla pois tuottavammasta työstä.

3.1.2 Ketteryys

Kuluttajistumistrendin myötä uutta teknologiaa pystytään ottamaan hyötykäyttöön aiempaa nopeammin. Tästä on erityisen suurta hyötyä aloitteleville yrityksille, joilla IT-infrastruktuuria ei ole vielä ehditty hankkimaan [McIlwain, 2011]. Tarvittavat laitteet ja erityisesti työlle tärkein rajapinta eli sovellukset on nykyisin vaivattomia ottaa käyttöön, erityisesti jos yritys on toimintansa alkuvaiheissa eikä menneisyyden infrastruktuurin painolastia ole mukana.

Toisaalta ilmiöstä voivat hyötyä myös vanhemmat organisaatiot. Tätä nykyä esimerkiksi uuden palvelukapasiteetin ostaminen verkon pilvipalveluista on tehty äärimmäisen helpoksi. Jos organisaatiolla ei ole erityisiä tietoturvasyitä, joiden vuoksi pilvipalveluiden hyödyntämistä tulisi jarruttaa, niin lisäkapasiteettia vanhalle konehuoneelle voi harkita ostavansa esimerkiksi Amazonilta tai Azuresta.

Sama käyttöönoton keveys koskee myös pilvestä saatavilla olevia muita sovelluksia. Jos vanhalla organisaatiolla esimerkiksi vanha varmistusjärjestelmä alkaa olemaan kallis ylläpitää ja huoltaa, niin ratkaisua voi hakea uudenlaisista varmistusratkaisuista kuten CrashPlanista, jolloin organisaatio voi halutessaan ja tietoturvan salliessa siirtää kokonaan varmistettavan datan pois omasta konehuoneesta. Tällöin mm. konesalikustannuksista voi saada merkittäviä säästöjä ja sovellukseen liittyvä tukipalvelu voidaan siirtää palvelutarjoajalle, jolloin tietohallinnon resursseja voidaan uudelleenohjata eri tehtäviin.

Jonkinlainen hyväksyntäprosessi ja ohjeistus tehtäville hankinnoille tulisi kuitenkin olla, jotta uuden teknologian omaksumisesta ei tulisi itsetarkoitus ja jotta uusien tekniikoiden tuominen osaksi organisaation kasvavaa kokonaisarkkitehtuuria olisi säänneltyä. Mikäli arkkitehtuuri on valmis ottamaan vastaan omien laitteiden ja uuden teknologian ketterän sulauttamisen osaksi organisaation infraa, voi parhaillaan organisaation uuden teknologian hyödyntäminen päästä samalle tasolle kuluttajamarkkinassa esiintyvän vauhdin kanssa [Willis, 2013].

3.1.3 Loppukäyttäjien työtyytyväisyyden ja motivaation kasvu

BYOD-mallia markkinoidaan usein siten, että loppukäyttäjien työtyytyväisyys ja työskentelymotivaatio saadaan nousuun, kun työkalut saa itse valita ja ne toimivat käyttäjän haluamalla tavalla. Gartnerin analyytikon, Bruce Willisin, mukaan BYOD:n kiistattomiin etuihin kuuluu uuden liikkuvan työvoiman avaamat mahdollisuudet ja kustannussäästöt. Mutta näiden lisäksi Willis listaa myös henkilöstön motivaation kasvun BYOD-ohjelmien käyttöönoton myötä [Willis, 2013].

Vastaavasti Accenturen vuonna 2010 tekemän kansainvälisen tutkimuksen mukaan, mitä enemmän työntekijöille annetaan mahdollisuuksia käyttää omaa harkintaa ja omia työkaluja työn tekemiseen, sitä enemmän tämä nostaa sekä motivaatiota että kykyä tehdä innovaatioita [Accenture, 2010].

Samalla tämä teknologisen kehityksen aallonharjalla matkustaminen voi tuoda myös etuja uusia ja usein nuoria työntekijöitä rekrytoitaessa. Accenturen mukaan jopa ¾ nuorista (18-27-vuotiaista) työnhakijoista antaa arvoa viimeisintä teknologiaa hyödyntäville

yrityksille – erityisesti jos rekrytoiva yritys antaa työntekijälle valtaa tehdä valintoja työkalujen suhteen. Maakohtaiset erot ovat kuitenkin suuria ja suurinta arvoa Accenturen tutkimuksen mukaan huipputeknologialle antavat intialaiset nuoret. [Accenture, 2010]

Erityisesti IT-alalla käyttäjät arvostavat mahdollisuutta käyttää uusimpia laitteita työtehtävien hoitamisessa. Vakioitu ja kaikille samanlainen työasema ei riitä, vaikka se usein kokonaisvaltaisesti kustannustehokkain ratkaisu olisikin.

Usein henkilöstön työtyytyväisyyskyselyissä on kohta, jossa kysytään tietoteknisten tukipalveluiden toiminnasta ja työkalujen toimivuudesta. Tällöin tietohallinto saa helposti pyyhkeitä kaikesta tietotekniikkaan liittyvästä toiminnasta. Loppukäyttäjät pitävät IT-toimintoja syyllisenä kun varsinainen ongelma voi olla käyttöjärjestelmässä tai liiketoiminnan omassa sovelluksessa.

Työtyytyväisyyskyselyissä tällaisen BYOD-mallin omiin valintoihin perustuvat teknologiavalinnat saattavat usein saada paremmat arvosanat, vaikka todellisuudessa omien laitteiden käyttäminen voi aiheuttaa samanlaisia tai jopa suurempiakin ongelmia työnteossa kuin organisaation valitsemat laitteet.

3.1.4 Vaikutukset tuottavuuteen ja innovaatioihin

Ajasta ja paikasta vapaa työntekijä voi tehdä töitä silloin, kun on tuottavimmillaan ja venyä esimerkiksi kotoa käsin suorituksiin, joihin työpaikalla ei välttämättä ehdi ja pysty. Tämä saattaa tarjota työnantajalle merkittävän edun, jos työntekijä voi itsenäisesti valita työaikansa perinteisen työajan ulkopuolelta.

Airwatchin [2012] mukaan myös työn tuottavuus paranee varsinkin matkaavien käyttäjien osalta, mikäli työskentelyyn käytetyt työkalut ovat tuttuja jo vapaa-ajalta.

Tuottavuuden kasvu ei kuitenkaan ole itsestään selvää. Parantunut motivaatio ja mahdollisesti käyttäjän kannalta paremmin tarpeisiin soveltuvat työkalut voivat kasvattaa tuottavuutta, mutta omien laitteiden käytön kääntöpuoli on se, että samoilla laitteilla tehdään sujuvasti myös henkilökohtaisia askareita. Tätä ei usein markkinointitarkoituksessa tehdyissä tutkimuksessa oteta huomioon. Omien laitteiden käyttö saattaa aiheuttaa myös häiriöitä tuottavuudelle, jos esimerkiksi itse hankitun tietokoneen ajuriongelmat ovat loppukäyttäjän riesana. Tällöin työntekijän aikaa saattaa kulua merkittävästi enemmän kuin

mitä osaavalta IT-tukihenkilöltä kuluisi tarkkaan vakioidun ja tuetun laitteen parissa ongelmanratkaisuun.

Erityisesti uusimpien teknologioiden parissa työskentelevät yhtiöt voivat hyötyä omien laitteiden käyttömahdollisuuksista huomattavasti. Organisaation kyky luoda ja tehdä uusia innovatiivisia ratkaisuita saattaa jopa kehittyä. Samoin organisaation omat toimintaprosessit saattavat parantua yllättävissäkin ympäristöissä, jos työntekijöitä kannustetaan kekseliäisyyteen omien laitteiden ja sovellusten käyttämisessä työn tekemiseen. [Harris et al., 2012]

Lisäämällä työntekijöiden vaikutusmahdollisuuksia, omien työkalujen käyttöä ja sallimalla erilaiset työtavat, voi henkilöstön työmotivaatio kasvaa ja uuden tekniikan avustamana uusien innovaatioiden syntyminen voi mahdollistua organisaation toiminnoissa, joissa perinteisillä työkaluilla ei uuden luominen onnistuisi [Accenture, 2010]. Nämä asiat voivat tuoda yrityksille merkittäviä kilpailuetuja.

Samoin omien laitteiden ja järjestelmien käyttöönoton myötä organisaatiossa voidaan ottaa käyttöön järkevämpiä ja taloudellisempia keinoja tehdä nykyistä työtä. Jos työntekijät seuraavat uusinta tekniikkaa ja työympäristö kannustaa siihen, niin uutta omaksumalla myös yhtiön omassa tuotekehityksessä voi tapahtua merkittäviä harppauksia verrattuna tilanteeseen, jossa organisaatio ei tietoisesti tue teknologisen osaamisen oma-aloitteista kehittämistä.

Tietohallinnon resursoinnin kannalta pilvipalveluiden hyödyntäminen voi vähentää ylläpitotyötä esimerkiksi IT-infrastruktuurin parissa tai vapauttaa sitä muihin tehtäviin. Toisaalta tämä infra-työ saattaa muuttua enemmän integraatio-osaamista painottavaksi, jotta uudet ostetut palvelut saadaan luonnolliseksi osaksi organisaation kokonaisarkkitehtuuria.

Pilvipalveluiden myötä myös organisaation data ja toiminnot liikkuvat helpommin mukana ja raja-aitoja asiakkaiden ja yhteistyökumppaneiden suuntaan voidaan kaataa. Esimerkkinä voisi mainita tilanteen, jossa ohjelmistoyrityksen työntekijän pitäisi julkaista 500 megatavun kokoinen päivitys asiakkaan (tai useamman) saataville. Tällainen jakelun nopea toteuttaminen sähköpostilla ei onnistuisi suuresta koosta johtuen. Eikä enää vuoden 2010 jälkeen ohjelmistopäivitysten jakaminen ole ollut järkevää muuten kuin tietoverkon

ylitse. Tällaista ohjelmistojakelua varten organisaation mahdolliseen FTP-palvelimeen tilapäisten tunnusten avaaminen sekä tunnusten ja salasanojen välittäminen voisi organisaation omat tietohallinnon prosessit huomioiden viedä useita päiviä. Sen sijaan esim. Dropboxin kaltaisella työkalulla jakelun saisi hoidettua helposti ja nopeasti suoraan – tiedosto pilveen ja linkin jakaminen sähköpostitse asiakkaille ko. tiedostoon riittäisi.

3.2 Esimerkkitapaus: Cisco

Suurista kansainvälisistä yhtiöistä Cisco on monella tapaa hyvä esimerkki siitä, miten kuluttajistuminen voidaan valjastaa hyötykäyttöön ja minimoida kuitenkin tästä aiheutuvat tietoturva ja muut riskit. Yhtenä vahvana syynä Ciscon tapaan rakentaa ympäristöä BYOD-aikakaudella lienee ollut Ciscon vahva teknologiaosaaminen.

Vielä vuonna 2007 Ciscon tietohallinto pyrki estämään kaikin tavoin OS X -laitteiden käytön yhtiön tietoteknisessä ympäristössä. Ciscolla oli vahva vakioitu Windows-pohjainen työasemaympäristössä käytössään, eikä sitä sotkemaan haluttu mitään ylimääräisiä laitteita. Cisco alkoi hyväksymään hiljalleen Mac OS X -koneiden käytön ympäristössään sillä ehdolla, että käyttäjät hoitivat itse Mac OS X -käyttöön liittyvät ongelmansa ja näiden koneiden tuominen organisaation tietoverkkoon ei saanut millään tavalla häiritä IT-toimintoja esimerkiksi tukipyynnöillä. Hiljalleen Ciscon ympäristöön ilmaantui yhä enemmän Mac-käyttäjiä, jotka alkoivat antamaan toisilleen vertaistukea ongelmissa. Vasta Applen iPhonen ja iPadin menestyksen myötä, Ciscolla alettiin ottamaan innolla Applen tuotteita vastaan ja tämän jälkeen myös IT-tuki Applen tuotteille alkoi järjestymään [Gruman, 2013].

Noin kuusi vuotta myöhemmin Ciscolla oli jo käytössä n. 35000 Mac-tietokonetta. Käyttäjät saavat valita nykyisin Windows-, Linux- ja OS X -koneiden väliltä. Applen iPhone, iPad ja OS X alkoivat muodostumaan hallittaviksi koneiksi IT:n näkökulmasta samoihin aikoihin kun Apple julkaisi Mountain Lion -version OS X -käyttöjärjestelmästä. Tämän myötä Applen tietokoneet alkoivat noudattamaan samaa rajapintaa asetusten hallitsemiseksi kuin mitä iPhone ja iPad -puolella oli tarjolla. Sittemmin jokaisen OS X -käyttöjärjestelmäversion myötä on tätä hallintarajapintaa edelleen kehitetty.

Koska hallintarajapinta on kehittynyt ja samoja määrityksiä pystytään nykyään asettamaan niin iOS- kuin OS X -laitteille, niin useat MDM-ratkaisut ovat myös alkaneet tukemaan suoraan Mac OS X -käyttöjärjestelmiä – kuten myös tuoreita Windows-käyttöjärjestelmiä. Tällä tavalla IT-ylläpitäjille on mahdollista saman MDM-tuotteen kautta hallita keskitetysti Windows- ja OS X -työasemia sekä lukuisia mobiililaitteita. Näin meneteltiin myös Ciscolla, jolloin monimutkaisen ympäristön hallinta helpottui merkittävästi.

Ciscon tapauksessa siirtymää iOS:n, OS X:n ja myöhemmin myös Linuxin käyttöön helpotti huomattavasti organisaation runsas Web-sovellusten käyttö. Suuri osa www-selaimen päällä toimivista sovelluksista on alustariippumattomia, joten valtaosa liiketoiminnalle tärkeistä ominaisuuksista saatiin toimimaan laitteessa kuin laitteessa. Ainoastaan vanhemmat sovellukset, jotka nojasivat ActiveX:n ja vanhojen Internet Explorer -selainversioiden varaan, tuottivat haasteita ja joidenkin vanhojen sovellusten vuoksi alkuun jouduttiin hyödyntämään Windows-virtuaalikoneita, joka ei ollut käytettävyyden näkökulmasta optimitilanne. Kokonaisten virtuaalikoneiden heikko käytettävyys ajoi joitakin sovelluksia päivittymään tavallista nopeammassa tahdissa alustariippumattomaan suuntaan.

Tallennusratkaisuissa Cisco oivalsi nopeasti sovellusympäristöä tarkkailemalla, että organisaatio tarvitsee käyttöönsä oman IT:n hallitseman pilvitallennusratkaisun. Organisaatiossa alettiin perinteisen pilvitallennuskiellon sijaan markkinoida Ciscon omaa pilvitallennusratkaisua. Ympäristössä otettiin myös käyttöön organisaation omat sovelluskatalogit, joista IT:n hyväksymiä ja suosittelemia sovelluksia saatiin käyttäjien laitteille.

Ciscon kaltaiselle suurelle tietotekniikkatalolle kuluttajistumisen hyötynäkökulmat ovat selvät. Cisco pystyy laajan alustatukensa kautta pysymään usealla rintamalla tekniikan aallonharjalla, mikä voi antaa merkittäviä kilpailukykyetuja muihin konservatiivisempiin kilpailijoihin nähden – samalla pitäen loppukäyttäjät tyytyväisenä tietohallinnon toimintaan ja kehittämällä sisäisesti osaamista, mistä voi olla hyötyä omien tuotteiden myynnissä ja tuotekehityksessä [Gruman, 2013;Anderson, 2014].

4 KULUTTAJISTUMISEN ONGELMAT ORGANISAATIOLLE

Tässä luvussa tarkastellaan organisaation kohtaamia ongelmia. Ne on jaoteltu seuraavissa kohdissa teknisiin, hallinnollisiin, tietoturvallisuuteen ja henkilöstön osaamisiin liittyviin näkökulmiin.

4.1 Tietoteknisen infrastruktuurin monimutkaisuuden kasvu

Omien laitteiden käyttöönoton myötä tyypillisesti organisaation tietotekninen ympäristö muuttuu aiempaa monimutkaisemmaksi. Seuraavissa alakohdissa tarkastellaan erikseen mobiilaitehallintaa, työasemien kytkemistä osaksi organisaation it-infrastruktuuria, verkkoihin liittyviä haasteita ja vanhasta sovellusarkkitehtuurista johtuvia ongelmia.

4.1.1 Mobiililaitteiden määrän kasvu ja hallinta

Mobiilaitekannan monipuolistuminen aiheuttaa sen, että suuressa organisaatiossa mobiililaitekanta pitää saada keskitetyn hallinnan piiriin. Tämä ei ole pelkästään turvallisuusasia. Laajan mobiililaitekannan valvonta ja ylläpito vaativat resursseja ja mikäli organisaatio ei sijoita infrastruktuuriratkaisuihin, jotka tukevat tätä toimintaa, niin tietohallinto, tukitoiminnot ja loppukäyttäjät painivat samojen ongelmien kanssa toistuvasti ja työaikaa kuluu automatisoitavissa oleviin toimintoihin. Siinä sivussa organisaation tietoturva voi rapistua.

Jos yrityksellä ei ole ennestään BYOD-trendiä tukevaa infrastruktuuria kuten mobiililaitteiden hallintajärjestelmiä (MDM) ja pitkälle vietyjä työasemien hallintasovelluksia (esim. AD ja SCCM[21]) sekä verkonvalvontaa (esim. 802.1X[22]), niin uudet investoinnit, laitteiden ja ohjelmistojen konfiguroinnit sekä järjestelmien käyttöönotto ja ylläpito voi-

[21] http://en.wikipedia.org/wiki/System_Center_Configuration_Manager (31.1.2015)
[22] http://en.wikipedia.org/wiki/IEEE_802.1X (31.1.2015)

vat tulla erittäin kalliiksi. Myös IT-henkilöstön kouluttaminen uusien järjestelmien käyttäjiksi voi aiheuttaa merkittäviä kuluja ja mahdollisten lisäresurssien palkkaamiseltakaan ei aina voida välttyä.

Mikäli MDM:n käyttöönottoa ei harkita, niin käytännön vaihtoehdot ovat hyvin rajalliset. Yhtenä vaihtoehtona on myöntää täysi päätelaitevapaus, jolloin kaikki hallinta, vapaus ja samalla myös vastuu jätetään loppukäyttäjille. Turvallisuutta voidaan tällöin lisätä pakottamalla käyttäjät luvitettuihin laitteisiin ja menetelmiin (kryptaus, pakotettu suojakoodi, yms.). Tällöin myös käyttäjät tulisi sitouttaa sovittuihin käytäntöihin. Toisessa äärilaidassa on täysi älypuhelimien käyttökielto organisaation tietojärjestelmissä. Yksinkertaisimmillaan tämä onnistuu verkkoteknisesti estämällä tunnistamattomien laitteiden pääsyn yrityksen verkkoon ja esimerkiksi koko mobiililaitetuen poistaminen käytöstä protokollatasolla organisaation sähköpostijärjestelmästä.

Jonkinasteisen kevyen hallintamahdollisuuden voi saada jo useiden sähköpostialustoiden mukana. Esimerkiksi IBM tarjoaa Lotus Notes -tuoteperheeseen IBM Notes Traveler[23] -palvelinohjelmistoa ja sovellusta, jolla voidaan hallita perustasolla mobiililaitteita ja saada näistä raportteja [IBM, 2010]. Tuotteen mobiililaitetuki on melko kattava ja useille mobiililaitteiden käyttöjärjestelmille löytyy suoraan Traveler-sovellus. Lisäksi uudet Travelerin versiot käyttävät myös ActiveSync-rajapintaa, jolloin esim. Applen iPhonen käyttö on mahdollista ilman erillistä puhelimeen asennettavaa Traveler-sovellusta.

Microsoft vastaavasti tarjoaa Exchange-ympäristöön ActiveSync-protokollaan pohjautuvia ratkaisuita. Omaan yritysverkkoon asennettu Exchange-ympäristö mahdollistaa hieman monipuolisemmat mahdollisuudet hallinnan räätälöintiin, mutta myös Office 365 -pilvipalvelun mukana saa älypuhelimia perustason hallintaan. Tällainen ratkaisu on kuitenkin erittäin rajoittunut ja vaatii ponnisteluja ja virittelyä pääkäyttäjiltä. Pelkän ActiveSync-politiikan ja mobiililaitteiden laitekohtaisten rajausten varaan rakentaminen ei vielä mahdollista kovinkaan kummallista ja helposti ylläpidettävää hallittavuutta. Mm.

[23] http://www-03.ibm.com/software/products/en/notetrav (31.1.2015)

mahdolliset raportit mobiililaitteiden käytöstä voi saada nykyisessä Office 365 -palvelussa käytännössä vain itse viritellyillä Powershell-skripteillä ja tällöinkin raportteihin saa todella rajoitetusti tietoa.

Office 365 -palvelun ylläpidolta saattaa jäädä myös huomioimatta OWA-sovellusten (Outlook Web Access) käyttö. Oletuksena palvelussa OWA-sovellukset ovat sallittuja ja koska OWA-laitteilta ei edellytetä mitään organisaation tietoturvakäytäntöjen käyttöönottoa tai laitteen rekisteröintiä, niin tällaiset laitteet ovat tietoturvallisuuden kannalta erittäin ongelmallisia. OWA-sovellus on saatavissa ilmaiseksi esim. perheen yhteiseen iPadiin, ja jos OWA-laitteiden käyttö on mahdollistettu palvelussa, niin tällaisen yhteiskäytössä olevan suojaamattoman laitteen käyttö voi olla ongelmallista.

ActiveSync-protokollan avulla sovellusrajoituksien rakentaminen jättää niin ikään toivomisen varaa, vaikka periaatteessa protokollaan on ko. ominaisuuksia jonkin verran määritelty. Sen avulla ei myöskään saada aikaan esim. organisaation hyväksymien sovellusten jakelua laitteisiin.

ActiveSync-protokollan suurimmat ongelmat liittyvät kuitenkin valmistajakohtaisiin toteutuksiin ja laitevalvontaan. ActiveSync-toteutukset eroavat valmistajakohtaisesti toisistaan paljon [Wikipedia ActiveSync, 2013]. Vaikka ActiveSync-protokollan avulla voidaan määritellä todella paljon asioita, niin protokollalla ei kuitenkaan voida valvoa sitä, kuinka hyvin jokin yksittäinen laite toteuttaa protokollan vaatimuksia.

Yleispätevästä kaikkia laitteita koskevasta ActiveSync-politiikasta tulee helposti todella löyhä kokonaisuus, jolla ei ole turvallisuuden kanssa juurikaan tekemistä. Toinen vaihtoehto on luoda esim. laitemallikohtaisia kovennettuja käytäntöjä, jolloin nimettyä laitemallia vasten luodaan sellainen ActiveSync-politiikkakokoelma, jota laite todennetusti tukee. Esimerkiksi Nokia E7 tuki vielä koko laitteen salaamista, mitä useat tämän päivänkään laitteet eivät suoraan ActiveSync-protokollan komentamana tue. Tietämällä tai opettelemalla laitemallikohtaiset rajoitukset tietohallinto voi rajata esim. sähköpostin liitetiedostojen käsittelyn mahdolliseksi ainoastaan laitteilla, jotka tukevat laitteen tallennusmuistin salaamista. Tämä kuitenkin edellyttää laitemallikohtaisia käytäntöjä, joiden suunnittelu, testaaminen ja ylläpitäminen ympäristön vaatimusten ja mobiililaitteiden käyttöjärjestelmäpäivitysten myötä vaatii resursseja. Android-leirissä erityisesti ActiveSync-

käytäntöjen noudattaminen on erittäin kirjavaa ja tästä syystä tietohallinnolle tulee helposti kiusaus sallia ainoastaan harvojen testattujen laitteiden käyttö organisaation sähköpostin lukemisessa.

Toinen suuri ActiveSync-protokollan ongelma on se, että pelkästään ActiveSync-protokollan avulla ei voida valvoa laitetta siinä määrin, että tiedettäisiin, onko laite murrettu (engl. rooted / jailbreak). Tällaisilta murretuilta laitteilta tulisi ehdottomasti estää pääsy yrityksen IT-infraan. ActiveSync-protokollan avulla tällainen valvonta ei kuitenkaan ole mahdollista.

Näillä perinteisillä ActiveSync-protokollaan pohjautuvilla tavoilla saadaan kyllä kustannukset pidettyä ainakin näennäisesti pieninä, mutta samalla älypuhelimien täysi kapasiteetti ja ominaisuudet eivät tule hyödynnetyksi optimaalisella tavalla. Perinteisempi eiälypuhelin voi riittää hyvin pelkän sähköpostin ja kalenterin käyttöön.

Täysiverisellä MDM-ratkaisulla sen sijaan saadaan huomattava määrä lisäominaisuuksia ja mahdollisuuksia mobiililaitteiden hallintaan. Pitkällä aikavälillä MDM-ratkaisuun sijoittaminen voi tuoda säästöjä ylläpitäjien työajassa ja tietoturvallisuuteen liittyvien riskien hallinnassa.

Markkinoilla on saatavilla lukuisia kilpailevia MDM-toteutuksia – Gartnerin arvion mukaan n. 60 toimijaa [Jeffrey, 2011]. Kuva 5 kertoo Gartnerin näkemyksen vuoden 2013 merkittävimmistä MDM-tuotteista.

Kuva 5. Vuonna 2013 markkinoilla olleita merkittäviä MDM-tuotteita [Redman et al., 2013; Willis, 2013]

Markkinajohtajat, kuten AirWatch (jonka VMWare osti vuonna 2014), ovat olleet markkinoilla jo yli kymmenen vuotta. Parhaimmillaan MDM-tuotteet tarjoavat todella laajan ominaisuuslistan:

- laaja alustatuki (iOS, Android, Windows Phone, Blackberry, Windows 8.1, OS X),
- turvallisuuteen liittyvien asetusten hallinta ja monitorointi,
- hallitut ja turvalliset työtilat (esim. turvallinen selain ja sähköpostiohjelma erillisenä muusta järjestelmästä),
- puhelimen ja/tai muistikortin suojaaminen ja salakirjoittaminen,
- sovelluskatalogi ja organisaation valitsemien sovellusten (myös omien) jakelu,
- hyväksymismenetelmät uusille sovelluksille,
- sovellusten mainetarkistukset sovelluskatalogin hallinnan tueksi,
- sovelluspaketointi / virtualisointi,
- valvontatyökalut,

- MEM / Mobile Expense Management – mm. datasiirtomäärien ja siten kustannusten hallinta,
- pitkälle automatisoitu tai avustettu mobiililaitteen käyttöönotto,
- tukipalvelut / itsepalveluportaalit,
- etähallinta,
- etänä suoritettavat laitteiden lukitsemiset,
- laitteiden tyhjentämiset joko koko laitteelle tai valikoidusti ainoastaan organisaation dataa koskeviin sisältöihin, ja
- sijaintiin perustuvat palvelut (esim. eri asetukset maantieteellisen sijainnin mukaisesti).

Markkinajohtajien MDM-tuotteet mahdollistavat myös hallinnan tuomisen työasemainfrastuktuurin puolelle Windows- ja MAC-alustoille. Esimerkiksi AirWatch ja Fiberlinkin MaaS360 tarjoavat keskeisien mobiililaitealustojen lisäksi tuen Windows- ja OS X -käyttöjärjestelmille. Nämä nimenomaiset tuotteet myös toteuttavat em. listasta valtaosan ominaisuuksia, kattavat asetusmahdollisuudet, itsepalvelun, hallitun ja valvotun turvallisuuden ja selkeät raportit. Markkinoilla on viime aikoina tapahtunut paljon yrityskauppoja. Odotettavissa on, että markkinajohtajat, kuten VMWare, yhdistävät omien tuotteidensa mahdollisuudet osaksi ostettuja MDM-tuotteita [Oltsik, 2014].

Merkittävimmät MDM-tuotteet on saatavilla myös ilman sijoitusta omaan konehuoneeseen – pilvipalveluna. Hinnoittelultaan mobiililaitehallinnan ohjelmistot ostettuina pilvipalveluina voivat olla 0-60 euron hintaluokassa vuositasolla per käyttäjä. Maksullisiin palveluihin kuuluu usein myös vähintään englanninkielinen tukipalvelu ja erikseen maksamalla saadaan palvelut räätälöitynä avaimet käteen -periaatteella. Lisenssimäärien ja sopimuskauden pituuden kasvaessa suuremmat organisaatiot pystyvät usein neuvottelemaan volyymihinnan hankinnoille. Markkinajohtaja AirWatchin kattavin Blue-palvelu maksaisi esimerkiksi nykyisen listahinnoittelunsa mukaan n. 1000 mobiililaitteen ympäristöön vuositasolla melkein 60 000 euroa / alle 60 eur per käyttäjä vuodessa. Tällaiseen pakettiin saakin jo todella kattavat ominaisuudet sekä tukipalvelun, mutta samalla jokaiselle hankitulle mobiililaitteelle voi laskea MDM-lisenssin lisähinnan.

MDM-markkinatilanteen murroksen voi huomata myös Microsoftin Office 365 -palvelussa. Alkuun palvelu on tarjonnut ainoastaan rajoitetun hallinnan Exchange ActiveSyncin avulla, mutta Office 365 -palveluun ollaan tuomassa vuonna 2015 myös MDM-ominaisuuksia, joilla voidaan mm.

- rajata käyttäjän kopioi - liitä -toiminnot siten, että organisaation sovelluksesta kopiointi ei toimi käyttäjän omiin sovelluksiin,
- estää yrityssovelluksista kuvaruutukaappauksien ottamisen ja viemisen kuluttajapuolelle,
- rooli- ja ryhmäpohtaiset kohdennetut käytännöt – esimerkiksi talouspuolelle voidaan asettaa tiukemmat käytännöt kuin markkinointiin,
- selective wipe / enterprise wipe – pystytään rajoittamaan mahdollinen mobiililaitteen tyhjennys vain mobiililaitteessa oleviin organisaation datoihin ja jätetään loppukäyttäjän yksityiset sisällöt ennalleen,
- compliance check – pystytään tarkastamaan, että mobiililaite noudattaa organisaation määrittelemää MDM-käytäntöä. Jos mobiililaite ei enää noudata ohjeistuksia, niin se menettää oikeudet organisaation dataan, ja
- jailbreak protection – pystytään estämään esimerkiksi murretun iOS-laitteen käyttö.

Ongelmana Office 365 -palvelun tulevassa MDM-ratkaisussa on toistaiseksi se, että laitetuki rajoittuu alkuvaiheessa Android- ja iOS-alustoihin, eikä MDM tue näin ollen edes Microsoftin omia Windows Phone -laitteita.

Vastaavasti Google toi jo vuonna 2013 omia kevyitä MDM-ratkaisuitaan Googlen yritysasiakkaille tarkoitettujen työkalujen joukkoon [Weiss, 2013]. Nykyään Googlen MDM-ratkaisu tukee jo käytännössä kaikkia merkittävimpiä puhelimien käyttöjärjestelmiä (iOS, Android, Windows Phone, Windows Mobile, BlackBerry) ja ActiveSync-protokollan kautta myös marginaalituotteita.

MDM-ratkaisujen hinnaston toisesta ääripäästä voi mainita suomalaisen Miradore Online[24], joka on periaatteessa ilmainen ja sen ansaintalogiikka tulee perustumaan sovelluksen sisäisiin ostoihin. Kotimaisesta näkökulmasta heikkona puolena tässä oli pitkään se, että Windows Phone -tuki puuttui aluksi kokonaan. Sittemmin tuki Windows Phone 8 ja 8.1 -alustoille on tullut mukaan. Hallintamahdollisuudet ja raportointi ovat tässä tuotteessa olleet suppeita, mutta mikäli organisaation tietohallinnon budjetti on tiukalla, niin tällaisesta perustason tuotteesta voisi olla kuitenkin jonkun verran apua mobiililaitteiden hallinnan kannalta. Tuotetta myös kehitetään hyvää vauhtia. Miradore myös tarjoaa jo isommille organisaatioille varsin kilpailukykyisellä hinnalla laajempia ominaisuuksia kuten vuonna 2015 julkaistavaa organisaation valitsemien mobiililaitepolitiikkojen pakottamista laitteisiin.[Miradore, 2015]

Haasteita BYOD-trendi tuo erityisesti siksi, että tuettavan laitekirjon määrä kasvaa, mikäli tämä organisaatiossa sallitaan. Tämän vuoksi hyvin toimiva MDM-tuote yhdistettynä järkevällä tavalla hallittuun ja vakioituun työasemainfrastruktuuriin on IT-infrastruktuurin hallittavuuden perusedellytys BYOD-aikakaudella. Organisaation IT-infrastruktuurin pitää mahdollistaa pitkälle viety automaatio, hyvä hallittavuus ja käyttäjää ajatellen pitkälle viety itsepalvelumalli, jotta uuden laitteen käyttöönotto ei työllistäisi rutiinitehtävillä IT-tukea eikä myöskään loppukäyttäjää.

Oikein mitoitetulla ja organisaation tarpeita palvelevalla MDM-ratkaisulla voidaan rajoittaa tai jopa ratkaista kasvavasta mobiililaitemäärästä ja mobiililaitteiden erilaisuuksista aiheutuva hallittavuusongelma. Investointina arvokkaimmat ratkaisut ovat kalliita ja lisäksi toistuvia menoeriä, mutta jos mobiililaitteisiin halutaan tuoda aitoa valinnanvaraa loppukäyttäjille ja niillä halutaan myös tehdä organisaation työtehtävien kannalta muutakin hyödyllistä kuin sähköpostin, kalenterin ja osoitekirjan käyttöä, niin silloin tällaisien järjestelmien hankinta tulee olemaan harkinnan arvoista.

AirWatch [2012] näkee BYOD-ilmiön siten, että se jopa yksinkertaistaisi IT-infrastruktuuria. Tämä on kuitenkin mahdollista vain ideaalitapauksessa, jos yrityksessä ulkoistetaan kaikki hallinnointi työntekijälle itselleen ja ostetaan pilvestä palvelut, ja käyttäjä itse

[24] http://www.miradore.com/miradore-online/ (31.1.2015).

huolehtii kaikesta tuesta, ylläpidosta ja laitevaihdoista, niin AirWatchin näkemys voi olla lähellä. Kuitenkin hyvin usein puhdasta BYOD-mallia ei ole, vaan puhutaan jonkinasteisesta hybridimallista, jossa halukkaat pääsevät mukaan BYOD-ohjelmaan ja osa käyttää työnantajan tarjoamia työvälineitä. BYOD-malli edellyttää toimivan infrastruktuurin rakentamista ja järkevää arkkitehtuuria toimiakseen, ja harvoissa organisaatioissa nämä ovat valmiina omien laitteiden käyttöä ajatellen. Hybridimallissa joudutaan palvelemaan niin monen käyttäjän eriäviä tarpeita, että yrityksen infrastruktuktuurista tulee helposti raskas hallita ja hallintatyökalujen käyttöönotto vaatii sekä rahaa että osaamista.

Organisaatioissa mobiililaitteisiin liittyvät teknologiset valinnat lähtevät siitä, että ympäristössä pitäisi olla selkeä mobiililaitestrategia, jonka pohjalta käytännöt luodaan. Vasta kun nämä perusasiat ovat kunnossa, niin voidaan alkaa suunnittelemaan teknisiä ratkaisuja ongelmien ratkaisemiseksi, ja teknisten ratkaisuiden sanelemana ylläpitäjät voivat rakentaa organisaation strategiaa vastaavat määritykset saatavilla oleviin hallintatuotteisiin.

4.1.2 Omien tietokoneiden kytkeminen osaksi organisaation tietojärjestelmiä

Kuluttajistuminen koskee vielä valtaosin mobiililaitteita, mutta vähintään yhtä tärkeää on miettiä tämän trendin vaikutusta työasemavalintoihin. Suomalaisissa organisaatioissa on vielä valtaosin tarkasti vakioidut laitekannat. Suuremmissa organisaatioissa valmistaja- tai laitevalinnat tehdään usein vuosiksi eteenpäin. Tällä saavutetaan kustannussäästöjä, koska valmistajat myöntävät usein volyymialennuksia yrityksille ja yhteisöille.

Joissakin organisaatioissa on vallallaan jo CYOD-käytäntö, jota myös Peters [2008] suosittelee lieventämään vakioinnin aiheuttamaa valinnanmahdollisuuksien rajaamista. Tällöin käyttäjä voi valita tietohallinnon vakioimista työasemista omaan toimenkuvaan ja mieltymyksiin soveltuvan laitteen. Joissakin organisaatioissa valinta on täysin käyttäjän tehtävissä ja toisissa poikkeamat normaalista täytyy hyväksyttää esimiehillä. Tyypillinen valikoima voi sisältää vain pari mallia tai esimerkiksi kevyen kannettavan, peruskannettavan, tehokannettavan, perustyöaseman ja tehotyöaseman. Usein kaikki työasemamallit ovat saman valmistajan tuotteita [Peters, 2008].

Edellä mainittu käytäntö on erittäin yleistä organisaatioissa joiden IT-toiminnot on ulkoistettu jollekin palvelutalolle. Palvelutalot ovat jo vuosia tehneet työasemavakiointia ja tuotteistaneet tukitoiminnot pitkälle juuri tiukkaan vakiointiin ja tiukkoihin palvelusopimuksiin nojaten. BYOD-trendin mukana myös palvelutalojen toimintaan voi tulla muutoksia, kun asiakasympäristöissä aletaan toivomaan tukea myös omien laitteiden käyttöönotoille. Joitakin tuotteistettuja palveluita Suomestakin jo löytyy kuten Fujitsun Patja Easy [Fujitsu, 2012].

Myös käyttöjärjestelmävalmistajat ovat lähteneet BYOD-kehitykseen mukaan. Tämä on nähtävissä esimerkiksi Windows 8.1 ja Windows Server 2012 R2 -käyttöjärjestelmien mahdollistamissa uusissa ominaisuuksissa. Windows 8.1 ja Windows Server 2012 R2 tuovat mukanaan mm. *Workplace Join*[25] ja *Work Folders*[26] -ominaisuudet, jotka on luotu juuri Windows-käyttöjärjestelmien BYOD-skenaarioiden tukemiseksi [Microsoft, 2014b].

Workplace Join -toiminnon avulla on mahdollista liittää esim. kotikone yhtiön resursseihin ilman, että kone liitetään varsinaisesti yhtiön käytössä olevaan toimialueeseen. Käytännössä laite rekisteröidään käyttämällä vahvaa varmenteisiin nojaavaa tunnistautumista ja käyttäjän toimialuetunnuksia [Moody, 2013]. Rekisteröitymisen jälkeen laitteesta jää myös jäljet Active Directoryyn, jolloin tietohallinto saa kunnollisen kirjanpidon siitä, mitä laitteita organisaation resursseja pääsee käyttämään.

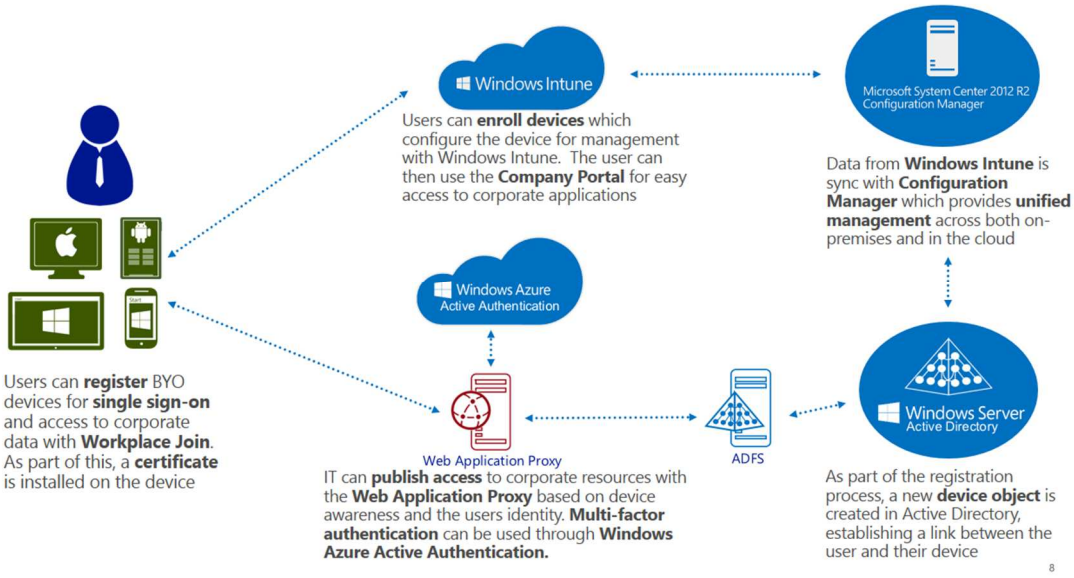
Sen lisäksi, että kevyellä toimialueeseen liittymisellä päästään käsiksi organisaation resursseihin, laitteella olevat tiedot voidaan jakaa yritysdataan ja yksityiseen dataan. Yritysdata ja yhtiön sovellukset voidaan poistaa koneelta etänä. Koko laitetta ei tarvitse tyhjentää. Joihinkin yritysympäristöihin ratkaisu voi olla omiaan lisäämään mahdollisuuksia kuluttajalaitteiden hyödyntämiseen. Ominaisuuden hyödyllisenä sivutuotteena myös alihankkijoina toimivien konsulttien työskentelyä osana organisaation infrastruktuuria pystytään tällaisella ratkaisulla helpottamaan, kun konsulteille ei välttämättä tarvitse järjestää toimialueeseen kytkettyä ja vakioitua työasemaa. Oikein käytettynä ominaisuus tuo myös

[25] https://technet.microsoft.com/en-us/library/dn280945.aspx (31.1.2015)
[26] https://technet.microsoft.com/en-us/library/dn265974.aspx (31.1.2015)

jonkinasteista turvaa yhtiön lisenssiomaisuuden hallitsemiseen, jos yksityiskäytössä olevat sovellukset pystytään erottamaan organisaation lisenssiomaisuudesta selkeästi.

Käyttäjänäkökulmasta Workplace Join -ominaisuudella voidaan myös tuoda mukava käytettävyyslisä single sign-on -toiminnon (SSO) mahdollistamana. Kertakirjautumisen avulla myös esimerkiksi iOS-käyttöjärjestelmällä varustettuja laitteita saadaan rekisteriin Active Directoryyn ja luvitettua käyttämään IT-infrastruktuurin mahdollistamia palveluita [Hester, 2013]. Lisäksi käyttäjän kannalta hyödyllisenä ominaisuutena voidaan pitää suhteellisen hyvin turvattua yksityisyyttä [Moody, 2013].

Kuvassa 6 on koostettuna Microsoftin Workplace Join -ominaisuuden uuden laitteen lisääminen osaksi organisaation Windows Server -ympäristöä.



Kuva 6. Worplace Join: laitteen rekisteröinti osaksi organisaation Windows Server-ympäristöä [Microsoft, 2014c].

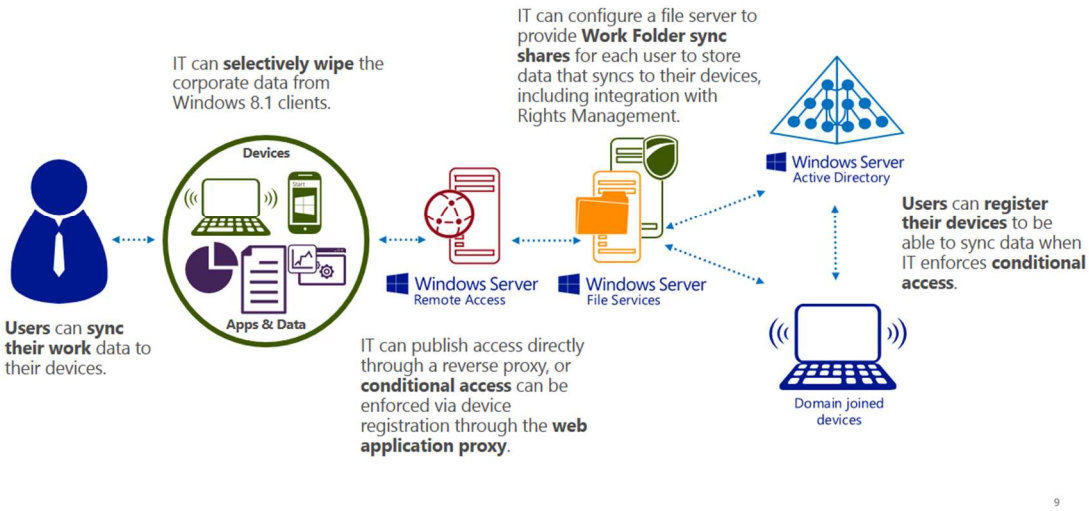
Hankaluutena Workplace Join -käyttöönotossa on se, että se vaatii olemassa infrastruktuurilta paljon. Käytännössä organisaatiolla pitää olla toimiva ajantasainen versio Active Directorysta, ADFS (Active Directory Federation Services) konfiguroituna ja lisäksi PKI-infrastruktuurin sekä siihen liittyvien prosessien pitää olla kunnossa. Mikäli esim. federointi-palvelut puuttuvat, niin ne täytyy ottaa käyttöön ennen kuin ominaisuutta voi harkita käyttöön [Hester, 2013]. Lisähankaluuksia tuo varmenteiden hallintaan liittyvä puoli.

Mikäli halutaan käyttää aitoja kuluttajalaitteita, niin varmenteiden pitää olla yleisiltä julkisilta varmentajatahoilta ostettuja, jotta voidaan varmistaa kuluttajalaitteiden luottaminen käytettyihin varmenteisiin.

Toinen merkittävä uusi ominaisuus on Work Folders. Work Foldersia voitaisiin luonnehtia omaksi organisaation sisäiseksi Dropbox-synkronointikansioksi. Work Folders -kansion avulla voidaan synkronoida käyttäjälle määritelty verkkosijainti Windows 8.1, Windows 7 tai Windows RT -koneeseen. Tämä toimii käyttäjänäkökulmasta perustoiminnoiltaan kuin Dropbox eli synkronisoitava kansio saadaan halutessa kaikkiin hyväksyttyihin käyttäjän laitteisiin. Organisaation tietoturvapuolta rauhoittamaan voi sisällön myös salakirjoittaa. Work Foldersin toiminnan runko on myös federointi-palveluissa ja toimivissa varmenteissa.

Windows Server 2012 R2 toi mukanaan myös uuden Web application proxy -palvelun [Remde, 2013]. Kyseinen palvelu toimii osana federointia ja mahdollistaa web-pohjaisten organisaation omien sovellusten julkaisun suoraan esimerkiksi rekisteröityneeseen iOS laitteeseen ilman vaivalloisen VPN-ratkaisun hyödyntämistä.

Kuvassa 7 esitetään Work Folders ja Web application proxy-palvelun mahdollisuuksia.



Kuva 7. Work Folders ja Web Application Proxy: käyttäjät pystyvät valitsemaan päätelaitteen halutessaan vapaasti ja pääsevät samoihin organisaation resursseihin käsiksi laitteesta riippumatta Microsoft, 2014c].

Vaikka omien koneiden kytkemiseen osaksi tietojärjestelmiä on alkanut ilmaantumaan erilaisia ratkaisuja, on se silti tietoturvanäkökulmasta edelleen haasteellista ja asia, johon

täytyy varautua huolella. Kokonaisarkkitehtuuri tulee rakentaa siihen kuntoon, ettei ympäristöön voi tuoda täysin vapaasti koneita ilman minkäänlaisia turvatarkastuksia. Uuden laitteen ympäristöön tuominen pitäisi lisäksi olla mahdollisimman pitkälle automatisoitu ja IT-tukea vähän kuormittavaa. Samoin poistuvista laitteista tulisi saada turvallisella ja todennetulla tavalla organisaation data ja lisenssit pois.

4.1.3 Verkkoon liittyvät haasteet

Laitteiden muuttuessa yhä enemmän langattomien verkkojen varassa oleviksi WLAN-verkon kapasiteetintarve kasvaa ja verkon tulee oltava huomattavan luotettava. Tietoliikennekapasiteetin uskotaan 26-kertaistuvan vuosien 2010-2016 välisenä aikana [Anderson, 2014]. Osa tästä kapasiteettikasvusta suuntautuu käytännössä melkein suoraan WLAN-verkkoihin (sekä yksityisiin, että julkisiin), vaikka osa mobiililaitteista jäisikin mobiiliverkkojen varaan [Jeffrey, 2011].

Suuressa liiketilassa siirtyminen WLAN-tukiasemien välillä pitää säilyä saumattomana, jotta tärkeimmät sovellukset jatkavat toimintaa myös liikuttaessa paikasta toiseen. Muussa tapauksessa sovellukset, jotka ovat riippuvaisia verkosta, voivat kaatua ja käyttökokemus heiketä.

Myös verkko-osoitteiden hallinnan kriittisyys kasvaa. Arvioiden mukaan verkossa olevien laitteiden määrä voi jopa nelinkertaistua nykyisestä, kun tyypillisellä työntekijällä ei enää ole pelkkää työasemaa vaan mahdollisesti useita muita mobiililaitteita [Anderson, 2014]. IPv6 tulee aikanaan ratkaisemaan suurempien laitemassojen käsittelyongelmat globaalistikin, mutta valtaosa organisaatioiden sisäisestä infrastruktuurista nojaa vielä vanhempaan IPv4 versioon, jolloin myös osoiteavaruuksien kanssa täytyy olla tarkempi.

Verkkoon liittyvä keskeinen haaste on myös verkossa olevien laitteiden hallinta ja valvonta. Verkkoon ei pitäisi päästää ylimääräisiä ja hallitsemattomia laitteita. Tässä IEEE 802.1x porttikohtainen todentaminen on hyvä ratkaisu, jolla pystytään tunnistamaan halutessa niin organisaation lähiverkkoon kytkeytyvä laite kuin käyttäjä [Wikipedia 802.1X, 2014b]. Mikäli organisaation lähiverkko (koskien sekä langallista ethernet-verkkoa että WLAN-verkkoa) toteuttaa 802.1x-standardia, niin verkkoon kytkettävien laitteiden hallinta saadaan kuntoon. Verkkoon liitetty todennettu laite ja käyttäjä pääsevät sisä-

verkkoon, mutta tunnistamattomat laitteet ja käyttäjät voidaan siirtää esim. DMZ-alueelle, jolloin osa verkkotoiminnoista voidaan jättää esim. ei-luotettujen vierailijoiden tai ei-hyväksyttyjen mobiililaitteiden käyttöön.

IEEE 802.1x mahdollistaa huomattavan parannuksen tietoverkon turvallisuudelle. Todentaminen yhdistettynä tietoturvatarkistuksiin esim. liitettävän työaseman tietoturvapäivitysten ja haittaohjelmasuojauksen osalta päästään jo varsin turvalliseen ja hallittuun tietoverkkoon.

Riippuen organisaation tarjoamien palveluiden laadusta ja tietoturvakriittisyydestä, voidaan joitakin portteja ulkomaailmaan jättää auki ja sallia esim. hallitusti federoinnin kautta joidenkin palvelujen käytön ilman raskaita VPN-yhteyksien perustamisia tai organisaation fyysisessä tietoverkossa vierailua.

Monien muiden BYOD-käyttöä helpottavien ominaisuuksien lisäksi Windows Server 2012 toi mukanaan uuden IP-osoitteiden hallintaa helpottavan ominaisuuden: DHCP Policy-Based Assignment (PBA)[Smith, 2012]. Tämän avulla DHCP-järjestelmänvalvoja pystyy määrittelemään organisaation verkko-osoitteiden jakoperusteet uusiksi siten, että esimerkiksi Applen valmistamat iOS-tuotteet saavat organisaation käytettävissä olevasta osoiteavaruudesta osoitteensa tietystä lohkosta. Tämän ominaisuuden mahdollistamana voidaan mm. hallita verkkoliikenteen priorisointia, määritellä verkko-osoitteilla rajattuja sovelluksia verkkoon ja varmistaa DHCP-ympäristön vikasietoisempi toiminta mm. sallimalla esimerkiksi organisaation tietoverkon sisällä toimiville pöytäkoneille erilaiset IP-osoitteiden uusiutumisajat kuin satunnaisesti verkossa vieraileville mobiililaitteille.

4.1.4 Vanhan sovellusarkkitehtuurin integroiminen uusiin ympäristöihin

Useissa vanhoissa organisaatioissa on vuosikausien aikana kertynyt runsaasti sovelluksia käyttöön, joiden elinikä voi olla hyvinkin pitkä. BYOD-aikakausi aiheuttaa tällaisiin ympäristöihin ongelmia, kun esimerkiksi vanhalle tuntikirjausjärjestelmälle ei välttämättä löydy hyvää mobiililaite-sovellusta tai www-käyttöliittymää.

Oman haasteensa päätelaitteiden monipuolistuessa tuo se, että erityisesti pitkään toimineiden organisaatioiden vanhojen liiketoimintajärjestelmien integroimisessa uusien päätelaitteiden käytettäväksi voi aiheutua ongelmia ja mahdollisia kokonaisten liiketoimin-

tajärjestelmien uusimisia mikäli vanha järjestelmä ei toimi uusilla käyttötavoilla. Virtuaalisilla työpöytäratkaisuilla (VDI)[27] pystytään ohittamaan joitakin tällaisia rajoituksia, mutta esim. virtuaalisen Windows-työaseman hallittavuus kosketusnäytölliseltä tabletilta ei ole nykytekniikalla erityisen käytännöllistä.

Toinen ongelma muodostuu näiden eri järjestelmien välisen integraatiotyön seurauksena. Alkuun BYOD-mallia hyödynnettäessä joitakin yksittäisiä sovelluksia, kuten sähköpostijärjestelmää, voidaan käyttää ongelmitta. Siinä vaiheessa kun halutaan myös vanhempia sovelluksia saada käytettäväksi uusilla laitteilla ja täysin uusien verkkoratkaisujen kautta, niin tietohallinto ajautuu helposti ongelmiin.

BYOD-mallin vetovoima perustuu sen yksinkertaisuuteen – yksinkertaista käyttöä, helposti ja ketterästi. Loppukäyttäjälle näkyvä sovellusten miellyttävä käyttökokemus voi kuitenkin niiden ratkaisujen rakentajille teettää kaikkea muuta kuin yksinkertaista työtä. Järjestelmäkokonaisuuksien kasvava monimutkaisuus vaatii erittäin hyvää kokonaisarkkitehtuurin hallintaa, runsasta suunnittelua ja kattavaa dokumentointia. Tähän ei välttämättä resurssipulasta kärsivä tietohallinto pysty.

4.2 Sopimus-, laki- ja lisenssitekniset asiat

Edellisten tekniikkaan liittyvien ongelmien lisäksi omien laitteiden hyödyntäminen tuo haasteita laki- ja sopimusteknisessä mielessä sekä sovellusomaisuuden hallinnassa. Tästä syystä organisaatioiden tulisi huolellisesti tarkastella ilmiötä, ei pelkästään tietohallinnon kannalta, vaan myös yhteistyössä lakiasiantuntijoiden ja henkilöstöhallinnon kanssa.

Henkilöstöhallinnon tulisi omien laitteiden käyttöä ajatellen suunnitella ja ylläpitää hallinnollisia prosesseja, joissa määritellään mm. korvausasiat omien laitteiden käytöstä. Henkilöstöhallinnon tehtäviin kuuluu myös mahdollisten roolien määrittely, mikäli organisaatiossa halutaan erilaisia BYOD-käytäntöjä henkilöiden työtehtävien mukaisesti.

[27] http://en.wikipedia.org/wiki/Desktop_virtualization#Virtual_desktop_infrastructure (31.1.2015)

Lakiasiantuntijoiden kanssa tulisi mm. selvittää työnantajan ja työntekijöiden oikeudet ja velvollisuudet muuttuneessa ympäristössä, jossa laitteiden ja ohjelmistojen omistajuus poikkeaa normaalista ”organisaation omaisuutta” -ajatusmallista. Koska kansalliset lait, verotus, asetukset ja sopimukset ovat jokaisessa maassa erilaiset, on näiden asioiden selvittäminen äärimmäisen tärkeää. Esimerkiksi monikansallisissa yrityksissä tulee kansalliset eroavaisuudet ottaa huomioon omien laitteiden käyttöstrategiaa suunnitellessa [Harris et al., 2012]. Myös vakuutusasiat tulisi tässä yhteydessä selvittää – korvaako organisaation vakuutukset esimerkiksi henkilöstön omien laitteiden varkaustapaukset vai tuleeko mahdolliset vakuutuskorvaukset hakea työntekijän omasta vakuutuksesta?

Erityisen tärkeää on kommunikoida loppukäyttäjille käytössä olevat omien laitteiden käyttöpolitiikat, jotta kenellekään ei jäisi epäselväksi esimerkiksi älypuhelimen kadotessa, mitä tietohallinto voi asialle tehdä (etätyhjennys). Tällaiset asiat tulisi selvittää etukäteen jo ennen oman laitteen käytön aloittamista, jotta vältyttäisiin asian lopulliselta selvittelyltä oikeussalissa. Vaikka kuluttajistuminen on ilmiönä vielä suhteellisen nuori, niin jo nyt on joitakin oikeusjuttuja nostettu vastaavanlaisten asioiden ollessa epäselviä [Anderson, 2014; Pervilä, 2013].

Kuluttajistuminen ja laajemmin ajatellen yhteiskunnan digitalisoituminen on lakia ajatellen erittäin haasteellinen ilmiö, koska kehitysvauhti on moninkertainen verrattuna siihen, miten lakeja on totuttu säätämään [Kasvi, 2014]. Lait ja asetukset eivät pysy teknologisten mahdollisuuksien perässä ja siksi lakiasiat saattavat tietyissä valtioissa jarruttaa merkittävästi kuluttajistumisen tuomia hyviä puolia. Esimerkiksi Saksassa on yksityisyyden suoja omien laitteiden käytön perustason valvontaakin ajatellen ongelmallinen, koska organisaatio ei Saksan lainsäädännön mukaan eroa yksityisyydensuojaa ajatellen juurikaan teleoperaattorista – mikä käytännössä suojaa käyttäjää kaikelta valvonnalta. Toisissa maissa, esimerkiksi Yhdysvalloissa, lainsäädäntö on kuluttajistumisilmiön kannalta huomattavasti käytännöllisempää IT-toimintojen järjestämisen kannalta [Harris et al., 2012].

Laki- ja sopimusasioiden lisäksi huomiota pitää suunnata ohjelmisto-omaisuuden hallitsijoille, jotka valvovat sitä, että organisaation käytössä olevien laitteiden ja sovellusten lisenssiehtoja noudatetaan. Varsinkin suurille organisaatioille auditointiriskit lisenssiehtojen laiminlyönneistä johtuen voivat olla valtavat. Useiden sovelluksien lisenssiehdoissa voi olla mainintana, että sovelluksen edelleen lisensointi ja allokointi ovat kielletty ilman

erillistä sopimusta sovelluksen valmistajan kanssa. Mikäli työntekijä käyttää omaa työasemaansa, johon asennetaan organisaatiolle lisensoituja sovelluksia, niin rajojen vetäminen lisenssiehtojen kannalta voi muodostua haasteelliseksi ja pahimmillaan seurauksena voivat olla mittavat korvaukset sovellustoimittajan suuntaan.

Jotkin sovellusvalmistajat ottavat BYOD-organisaatioiden onneksi jo kiitettävällä tavalla lisenssien liikkuvuuden huomioon. Esimerkiksi Adoben Creative Cloud[28] -ratkaisut ja Microsoftin Office 365[29] -lisensointimallit perustuvat käyttäjäkohtaiseen lisenssiin. Lisenssi voi liikkua käyttäjän mukana koneelta toiselle ja parhaimmillaan esim. Office 365 Pro Plus -paketin voi saada yhtiön työntekijänä asentaa lisenssiehtojen puitteissa jopa viidelle koneelle. Pilvipalvelu pitää lisensseistä kirjaa ja työsuhteen päättyessä ohjelmiston lisenssi ei enää uusiudu, jolloin sovellus ei enää toimi tai toimii rajoitetussa tilassa. Microsoft on kesällä 2014 laajentanut myös Office 365 Pro Plus -toiminnallisuutta siten, että organisaatiot voivat hyödyntää samaa pakettia ns. Shared Computer Activation[30] -tilassa, jolloin sama käyttäjä voisi käyttää sovellusta esim. kannettavassa, palvelimella remote desktop -istunnossa ja kotona. Aiemmin tällainen monen käyttäjän ympäristössä tapahtuva ko. sovelluksen käyttäminen ei ole lisenssiehtojen puitteissa ollut mahdollista. Shared Computer Activation mahdollistaa sen, että usean käyttäjän palvelimella sovellus on asennettuna kertaalleen, mutta aktivointi tapahtuu käyttäjäkohtaisesti, jolloin lisenssin haltijoilta varataan lisenssit ja sallitaan käyttö. Lisenssittömät eivät puolestaan pysty sovellusta käyttämään muuta kuin kokeilutilassa.

Vastaavasti vuoden 2014 joulukuussa Microsoft toi uuden Windows-käyttöjärjestelmien lisensointimahdollisuuden julki [Foley, 2014]. Uusi malli tuo omien laitteiden käyttöjärjestelmien puolelle samanlaisia mahdollisuuksia kuin Office 365 Pro Plus. Joillekin organisaatioille tämä voi tuoda jopa säästöjä, mutta koska lisensointimallit ovat erittäin monimutkaisia, niin asia ei ole aivan niin suoraviivainen. Siinä missä uusi malli voi joissakin ympäristöissä helpottaa lisenssien hallintaa, niin se voi myös tuoda lisäkustannuksia.

[28] http://www.adobe.com/fi/creativecloud.html (31.1.2015)
[29] http://products.office.com/en-us/office-365-home (31.1.2015)
[30] http://blogs.technet.com/b/uspartner_ts2team/archive/2014/09/03/office-365-shared-computer-activation.aspx (31.1.2015)

Microsoftin kannalta ajatuksena lienee vuokramallin laajentaminen myös Windows-käyttöjärjestelmien puolelle ja siten uusien ansaintamallien kehitys. Sivutuotteena organisaatiot voivat saada uusia mahdollisuuksia osaksi Microsoftin kanssa tekemiään sopimuksia.

Valtaosa sovelluksista lisenssiehtoineen ei kuitenkaan tue tällaista käyttäjäkohtaista lisensointia ja osassa lisenssiehtoja voi olla eksplisiittisesti mainittu, että ohjelmiston käyttö on sallittua vain yhtiön omistamilla koneilla. Koska lisenssiehdot ovat tavalliselle käyttäjälle erittäin haastavia ymmärtää, niin jonkinlainen hallittu ohjelmistojen hyväksyntäprosessi tulisi olla BYOD-politiikkaa noudattavassa organisaatiossakin käytössä, jotta räikeiltä lisenssien väärinkäytöiltä vältyttäisiin.

Koska lait, sopimukset ja lisenssit ovat kokonaisvaltaisesti todella haasteellinen osa-alue, niin BYOD-politiikan pitäisi myös huomioida nämä ja olla riittävän tarkkaan määritelty, jotta tulkinnanvaraisuuksilta voitaisiin välttyä. BYOD-politiikka pitää myös olla käyttäjille riittävän selkeä ja se pitäisi käyttäjien hyväksyä ennen omien laitteiden hyödyntämistä. Samoin BYOD-politiikkaa pitäisi katselmoida uudestaan esim. puolen vuoden välein, koska tekniikan kehittyessä tällaiset säännöt vanhentuvat helposti.

4.3 Tietoturva-asiat

Tietoturva on yleisesti keskeisin este omien laitteiden käyttöönottamiselle. Tietoturvakriittisimmät organisaatiot saattavat kieltää täysin omien laitteiden käytön työtehtävissä. Vaikka organisaation toimiala ei edellyttäisi korkeaa tietoturvatasoa, on näihin asioihin kuitenkin kiinnitettävä huomiota ongelmien ennaltaehkäisemiseksi. Seuraavissa alakohdissa pohditaan tietoturvahaasteita ensin yleisellä tasolla. Tämän jälkeen selvitetään laitteisiin ja sovelluksiin liittyvää tietoturvaa sekä tietoteknisen ympäristön valvontaa. Lopuksi selvitetään, mitä ongelmia liittyy pilvipalvelujen tietoturvaan.

Suurin huolenaihe omien laitteiden käyttöön ottamisessa on aina ollut tietoturva. Organisaatioiden infrastruktuuria on yleensä johdettu ylhäältä käsin ja pakotettu tietoturva-asetukset käyttöön kaikkiin organisaation keskitetysti hankkimiin, vakioimiin ja hallinnoimiin työasemiin. Sama käytäntö on koskenut älypuhelimia niiden ilmaantumisen alkuaikoina.

Kuluttajistumisen herättämät huolenaiheet eivät ole tuulesta temmattuja. Esimerkiksi Avanaden tilaaman tutkimuksen mukaan jo vuonna 2011 suuri osa kyselytutkimuksessa mukana olleista yrityksistä oli jo kokenut jonkinasteisen tietomurron kuluttajistumisen suorana seurauksena. BYOD-käytäntöjen yleistyessä tietoturvapolitiikat ja niistä seuraavat järjestelmien ja käytäntöjen kovennukset eivät ole pysyneet kuluttajistumisen tahdissa vaan seuranneet askeleen perässä. [Wakefield Research, 2012]

Omien laitteiden ja tekniikoiden käyttäminen osana organisaation tietojärjestelmiä on monellakin tapaa tietoturvanäkökulmasta ongelmallinen. Tietotekniikan parhaiden käytäntöjen mukaisesti on ollut tapana vakioida työasemat muutamaan tuettuun saman laitevalmistajan malliin sekä organisaation tarpeita riittävästi palvelevaan sovelluskatalogiin [Peters, 2008]. Vakioimalla ympäristö on voitu pienillä IT-resursseilla saavuttaa kevyellä vaivalla suhteellisen turvallinen, mutta samalla myös suljettu, järjestelmäympäristö.

Mobiililaitteiden ja pilviteknologian kehittyessä, verkkojen muuttuessa langattomiksi ja erilaisten BYOD-käytäntöjen myötä ajat kuitenkin muuttuvat. Mitä enemmän tietotekniseen ympäristöön tulvii erilaisia laitteita ja ohjelmistoja, niin seurauksena syntyy myös aivan uusia mahdollisia hyökkäysmahdollisuuksia organisaation tietojärjestelmiä kohti.

Hyvä esimerkki ongelmallisesta asiasta on kirjava mobiililaitekanta. Mikäli sallitaan minkä tahansa mobiililaitteen ActiveSyncin hyödyntäminen, niin tällöin myös oletusarvoisesti joudutaan tekemään todella kevyitä ActiveSync-käytäntöjä, koska päätelaitteiden ActiveSync-toteutukset eroavat rajusti toisistaan [Wikipedia ActiveSync, 2013]. Toinen vaihtoehto on luoda päätelaitekohtaisia käytäntöjä, mutta niiden räätälöiminen ympäristön tarpeisiin vaatii runsaasti työtä. Toisaalta taas liian liberaali käytäntö voi johtaa merkittäviin kompromisseihin tietoturvan osalta, mikä voi olla organisaatiolle iso riski. Kun kuluttajien älypuhelimet oletuksenakin jakavat runsaat määrät tietoa sosiaaliseen mediaan ja muihin verkkopalveluihin, niin organisaatioiden on oltava tarkkana siinä, kuinka tiukasti näitä laitteita sidotaan organisaation muihin tietojärjestelmiin vai sidotaanko ollenkaan. Näiden asioiden vuoksi kattavat MDM-ratkaisut tarjoavat IT-ympäristön ylläpitäjille huomattavaa helpotusta.

BYOD-innostuksessa jarrua painavat erityisesti tietoturvakeskeiset organisaatiot. Tällaisia ovat mm. terveydenhuollon, valtionhallinnon, viranomaistoiminnan ja armeijoiden sekä puolustusvälineteollisuuden organisaatiot. Näitä usein sitovat lait ja säännökset, jotka pakottavat noudattamaan tiukkoja tietoturva-asetuksia ympäristössään.

Suomessa Kansallinen turvallisuusauditointikriteeristö (Katakri II) rajaa esimerkiksi puolustusvoimien ja puolustusvoimien kumppaneiden mahdollisuuksia hyödyntää kuluttajistumisilmiötä osana toimintaansa. Katakrissa määritellyt tietoturvavaatimukset ovat niin tiukkoja, etteivät näitä kriteereitä noudattavat organisaatiot voi millään päästä BYOD-ilmiötä tietoteknisessä ympäristössään normaaliin tapaan läpi. [Katakri2, 2011]

Vastaavasti terveyden- ja sairaanhoidossa potilastietojen luottamuksellisuudesta johtuen ei potilastietoja voi käytännössä huoletta käsitellä ns. kuluttajalaitteilla. Kuitenkin maailmalla on esimerkkejä, joissa tiukkaa tietoturvaa noudattavissakin ympäristöissä keksitään keinoja kuluttajalaitteiden hyödyntämiselle. Esimerkiksi kuluttajamarkkinaan tarkoitettuja iPadeja voidaan käyttää sairaanhoidossa mm. streaming-tekniikkaa hyväksikäyttäen, jolloin laitteeseen ei itse asiassa tallenneta luottamuksellista terveystietoa, vaikka sitä näytöllä tarpeen tullen pystytäänkin näyttämään. [Harris et al., 2012]

Toisaalta kaikessa tietoturvakeskustelussa on huomioitavaa, että itse asiassa omia kotikoneita on käytetty työntekoon tavalla tai toisella jo vuosikaudet. Asiakirjoja on liikuteltu työpaikan ja kodin välillä paperilla, USB-tikuilla, sähköpostiliitteinä ja erilaisilla levykkeillä. Kotona on ennenkin voitu jatkaa siitä, mihin työpaikalla jäätiin. Sikäli jonkinasteinen työpaikan ja kodin tietokoneiden sekaympäristö on ollut käytössä jo pitkään useissa organisaatioissa, vaikka sitä ei halutakaan avoimesti myöntää ja useiden organisaatioiden tietoturvapolitiikka yksiselitteisesti kieltää tällaisen toimintatavan. Nykyisessä äärimmilleen verkottuneessa ympäristössä kuitenkin mm. tietovuotojen riskit ovat kasvaneet merkittävästi, koska tiedon jakamisesta ja saatavuudesta on tullut äärimmäisen helppoa.

Kun kuluttajateknologia tekee työtehtävien suorittamisesta entistä helpompaa, niin käyttäjiä tietoturvallisuudesta vastaavien vaatimat käytännöt, säännöt ja kovennukset lähinnä rasittavat. Harris Interactiven tekemän kyselytutkimuksen, jossa haastateltiin yli 900 yhdysvaltalaista työläistä, jopa puolet työntekijöistä suhtautui epäluuloisesti tietohallinnon vaatimuksiin tietoturvakäytäntöjen noudattamisesta. Suurin syy epäluuloon oli pelko oman yksityisyyden vaarantumisesta [Vijayan, 2014]. Tutkimuksessa käy myös ilmi, että toistaiseksi BYOD-politiikkaa ei ole pakotettu ja valvottu huolella. Esimerkiksi teknisiä pakotuskeinoja tietoturva-asetusten noudattamiselle ei useilla organisaatioilla ole käytössä. Lisäksi käyttäjien epäluuloisuus luotuja tietoturvaohjeistuksia kohtaan kertoo paljon organisaatioiden viestintäongelmista BYOD-politiikkaa jalkauttaessa. Pahimmillaan

epäluulot ja liian tiukat tietoturva-asetukset ja -säännöt voivat aiheuttaa myös omien laitteiden käyttämisen boikotointia työntekijöiden taholta [Vijayan, 2014].

4.3.1 Laitteiden tietoturva

Kuluttajistumisilmiön tietoturvapuolen keskiössä voidaan pitää laitteisiin kohdistuvaa tietoturvaa. BYOD-ilmiön keskeisenä teemana ovat usein mukana kulkevat laitteet – kannettavat tietokoneet ja älypuhelimet. Liikkuvuuden myötä organisaation perinteinen fyysinen tilaturvallisuus ei koske usein mobiililaitteita, joita voidaan käyttää lentokentillä, kahviloissa, kotona ja asiakkailla. Liikkuvuudesta aiheutuu riskejä, koska pienet älylaitteet ovat helppoja hukata ja mobiililaitteet ovat helposti varastettavia. Mitä enemmän heikosti suojattuja ja kryptaamattomia laitteita häviää, sitä aiemmin tulee tiukennuksia tietoturvapolitiikkaan.

Organisaatioiden kannalta olennaista liikkuvien laitteiden turvallisuuden takaamiseksi on kryptata olennaiset ja arkaluontoiset tiedot sekä varmistaa laitteen kadotessa tai työsuhteen päättyessä organisaation tietosisältöjen turvallinen poistaminen. Datan poistotoiminnoissakin voi olla useita tasoja. Voidaan puhua ns. erikseen organisaatiodatan poistosta (engl. selective wipe / enterprise wipe), jolla poistotoimenpiteet voidaan kohdistaa ainoastaan organisaation dataan ja jättää esimerkiksi käyttäjien yksityiset tiedostot jäljelle. Tällöin puhutaan yleensä esimerkiksi organisaation hallinnassa olevan sähköpostitiliin liittyvän tiedon poistamisesta, mutta edistyksellisemmissä ratkaisuissa poistot voidaan laajentaa myös koskemaan muita organisaation omia sovelluksia ja näiden informaatiosisältöjä. Toinen vaihtoehto laitteen tyhjennykselle on koko laitteen alustaminen tehdasasetuksiin (engl. wipe). Tässäkin on valmistajakohtaisia eroja. Toisissa laitteissa tyhjennys on yksinkertaisempi ja toisissa laitteissa poisto voi suorittaa turvallisemman ylikirjoituksen laitteen tallennustilaan.

Koska kadonneiden ja käytöstä poistuvien laitteiden tyhjennys on olennainen osa organisaatioiden arkea ja tyhjennyskäytäntöihin on useita erilaisia tapoja ja tekniikoita, tulisi loppukäyttäjille viestiä tarkoin tietohallinnon tekniset mahdollisuudet tyhjennystoimille ja politiikat milloin mitäkin tyhjennysmenetelmää käytetään. Tämä olisi olennaista viestiä jo laitteita käyttöönotettaessa, jottei IT:n ja loppukäyttäjien näkemyksiin pelisäännöistä muodostuisi eroja.

Joissakin organisaatioissa vaaditaan lisäksi esimerkiksi työasemien ja mobiililaitteiden tyhjennyksistä tarkkoja lokitietoja auditointitarkoituksia varten, jotta voidaan varmentaa, että tyhjennykset on suoritettu sovituilla tekniikoilla ja datanpalautus ei ole enää mahdollista. Tällaisissa tilanteissa poistuvan laitteen tyhjennystä ei voi jättää pelkästään käyttäjän omatoimisuuden varaan, vaan tyhjennys pitää suorittaa tarkoitukseen kehitetyllä ja hyväksytyllä sovelluksella säilyttäen lokitiedot tyhjennystapahtumasta tallessa. Tällaisissa skenaarioissa valikoiva laitteen tyhjennys ei yleensä ole mahdollinen.

Olennaista organisaatioiden osalta on myös lisenssien poistaminen niiltä koneilta, joilla lisenssiä ei enää tarvita. Esimerkiksi arvokkaiden CAD-sovellusten unohtaminen käyttäjän omalle koneelle työsuhteen päätyttyä voisi tulla todella kalliiksi organisaatiolle.

MDM-tuotteet ovat tyypillisiä esimerkkejä siitä, miten monenlaisten laitteiden (myös muiden kuin Windows-tietokoneiden) tietoturvaa voidaan koventaa. Tämä ei yleensä vielä riitä, vaan myös sovellusten tietoturvaan tulee kiinnittää kuluttajistumisilmiön osalta huomiota [Scarfò, 2012].

4.3.2 Sovellustietoturva

Microsoft Security Intelligence Report vuodelta 2013 mainitsee yhtenä suurena tietoturvahaasteena sovellusmäärän valtavan kasvun [Microsoft, 2013]. Mitä enemmän erilaisia ohjelmistoja on tietokoneilla ja mobiililaitteilla, sitä haastavampaa on sovellusten ylläpitäminen, päivitysten jakelu sekä sovellusversioiden hallinta ja valvonta. Microsoftin raportin mukaan valtaosa haavoittuvuuksista tällä hetkellä liittyy ohjelmistoihin – ei niinkään enää varsinaiseen käyttöjärjestelmään tai www-selaimeen. Tyypillisiä haavoittuvia komponentteja tietokoneiden puolella ovat Java Runtime Environment, Adobe Flash ja PDF-lukijat.

Jos sovelluskirjo on valtava, niin usein myös sovellusten vanhojen versioiden häntä jää roikkumaan ja verkossa saattaa olla hyvinkin vanhoja, päivittämättömiä, sovellusversioita, joissa saattaa olla merkittäviä tietoturvahaavoittuvuuksia. Sovelluksia ei välttämättä päivitetä keskitetysti, hallitusti ja ajallaan. Tällaisessa tapauksessa yksikin pahasti haavoittunut kone voi olla reitti hyökkäykseen.[Microsoft, 2013]

Toisaalta BYOD-kulttuurin mukana tuleva käyttäjien valta valita mahdollistaa heterogeenisemman sovellusvalikoiman. Tästä voi joissakin tapauksissa olla tietoturvan kannalta

myös etua, koska laajan kohdennetun hyökkäyksen tekeminen on vaikeampaa, jos esimerkiksi organisaatiossa on käytössä useita eri valmistajien PDF-lukijoita. Mikäli organisaation sovelluskirjo on heterogeenisempi, niin yksittäisten sovellusten haavoittuvuuksien hyödyntäminen koko organisaatiota vastaan on vaikeampaa, kun hyökkäyspinta-ala on pienempi.

Mikäli organisaatiossa osana BYOD-politiikkaa tuodaan vapauksia myös sovellusten valintaan ja käyttäjien omakohtaisiin asennuksiin, niin tilanteen hallinnan kannalta IT-infrassa tulisi mielellään ottaa käyttöön joku sovellusten sallimista / estämistä tukeva järjestelmä. Tällaisia White list / Black list -tyyppisiä ratkaisuja tarjoaa esimerkiksi Microsoftin Applocker[31] ja vielä kattavampi Avecto Priviledge Guard [Avecto, 2013], joka tätä työtä kirjoittaessa oli uudistunut Defendpoint[32]-nimiseksi tuotteeksi tammikuussa 2015. Tällaisilla sovelluksilla on mahdollista sallia (white-list) tai estää (black-list) nimettyjen sovellusten suorittaminen kokonaan. Vaikka esimerkiksi Windows-infrassa on ollut mahdollista myös ryhmäkäytännöillä (engl. Group Policy) rakentaa estoja, niin näillä asiaan erikoistuneilla sovelluksilla voi saada kasvavan sovelluskatalogin tehokkaasti hallintaan ja samalla pakottaa organisaation määrittelemiä suojauksia tehokkaasti käyttöön työasemaympäristössä.

Sovellustietoturvaa voidaan lisäksi parantaa liikkuvien laitteiden kannalta mm. virtualisointi ja streaming-tekniikoilla, jolloin esimerkiksi tabletissa ei koskaan varsinaista organisaation informaatiota käsitellä, mutta sitä toistetaan virtualisoidusta ja kovennetusta ympäristöstä – usein suoraan esimerkiksi organisaation omasta konehuoneesta. [Scarfò, 2012]

4.3.3 Seuranta

Tietojärjestelmien toimivuuden, organisaation prosessien ja työntekijöiden toimien, riittävä, mutta samalla yksityisyyttä ja lakeja kunnioittava seuranta (*engl. audit*) on yksi tietojärjestelmien pitkäaikaisen toiminnan perusedellytys.

[31] https://technet.microsoft.com/en-us/library/dd723678(v=ws.10).aspx (31.1.2015)
[32] http://www.avecto.com/defendpoint (31.1.2015)

Teknistä auditointia tai seurantaa voisi verrata terveystarkastukseen. Terveystarkastuksenkin idea on varmistaa, että kaikki on kohteessa hyvin. Tilanteissa, joissa kaikki ei ole hyvin, pitäisi pystyä jäljittämään, mistä syystä tilanteeseen on tultu. Tällä tavalla myös korjaustoimenpiteet voivat olla mahdollisia. Sama koskee tietojärjestelmiä – auditoinnin tarkoituksena on mm. varmistaa, että tietoteknisessä ympäristössä tiedetään mm. seuraavat asiat [Fox, 2012]:

- kenellä on pääsy tietoteknisiin resursseihin ja mistä näihin resursseihin on pääsy (sisäverkosta, VPN-yhteyden yli, intranetin kautta, pilvipalvelun kautta tms.),
- kuka tai mikä liikennöi verkossa ja käsittelee dataa – ja milloin, ja
- tietoteknisen ympäristön konfigurointi ja siihen tehdyt muutokset ajan kuluessa.

Näiden tietojen perusteella voidaan tietoteknistä ympäristöä kehittää, parantaa sekä suojata organisaation dataa entistä paremmin. Lisäksi toimivan seurannan avulla ongelmatilanteissa on mahdollista selvittää, mikä on mennyt pieleen. Vasta tämän tiedon avulla voidaan tilanteesta kunnolla toipua ja mahdollisesti myös muuttaa ympäristöä siten, että tilanne ei pääse toistumaan.

Tekninen auditointi perustuu pitkälti erilaisten lokilähteiden ja konfiguraatioiden seurantaan. Seuranta voi olla reaktiivista, jolloin yleensä lokeja aletaan tutkimaan vasta siinä vaiheessa, kun jokin tilanne on esiintynyt jotain muuta kautta. Seuranta voi olla myös proaktiivista. Tällöin esimerkiksi automaattinen lokienkeruujärjestelmä voi hälyttää ylläpitoa esimerkiksi haittaohjelmalle tyypillisen verkkoliikenteen havaitsemisesta tai jonkun käyttäjän tunnuksiin kohdistuvasta liiallisista kirjautumisyrityksistä.

Pelkkä tekninen auditointi, lokien kerääminen ja tapahtumiin reagoiminen ei tyypillisesti riitä. Tietojärjestelmiä pitäisi kehittää ja valvoa säännöllisesti, jotta esimerkiksi vuosien kuluessa erilaisista teknisistä konfiguraatio- tai organisaation toimintatapamuutoksista ei aiheutuisi organisaation toiminnalle ylimääräisiä riskejä.

Kuluttajistumisen myötä erilaisten seurantamenetelmien ja auditointien tarve tulee luultavasti kasvamaan huomattavasti, koska toimintaympäristö muuttuu monimutkaisemmaksi ja tietoturvan kannalta uusia riskitekijöitä ilmaantuu lisää. Liikkuvia laitteita myös vierailee verkossa yhä enemmän, jolloin seurannan arvo nousee entisestään.

Joiltakin organisaatioilta lisäksi edellytetään esimerkiksi jonkin auditointikriteeristön noudattamista. Tällaisissa ympäristöissä kuluttajistumiseen liittyvien aspektien tarkastelu on erityisen tärkeää.

4.3.4 Pilvipalvelujen tietoturva

Pilvipalveluiden nopea ja laaja levittäytyminen kuluttajamarkkinaan on alkanut nopeasti vaikuttamaan myös organisaatioiden IT-osastojen arkeen. Verkkotallennuspalveluita, sähköpostisovelluksia, ryhmätyötiloja ja muita äärimmäisen käteviä palveluita saa vaivatta verkosta. Usein vieläpä yleisien tietoliikenneporttien kautta, jolloin organisaatiot ovat vaikeuksissa, koska tällaisien pilvipalvelujen estäminen organisaation tietoverkosta etukäteen voi olla haastavaa.

Pilvipalvelujen tietoturva herättää syystäkin huolta. Tietohallinnot ovat vuosien saatossa tottuneet tilanteeseen, jossa organisaation tieto on valtaosin tallessa omassa konehuoneessa, varmistusnauhoilla ja organisaation palomuurilla rajatun tietoverkon sisällä. Lisäksi ylläpitohenkilöstön on pystynyt usein nimeämään. Pilvipalveluiden aikakaudella tilanne on toinen. Työntekijät voivat hyödyntää yksityisiä sähköpostilaatikoitaan, verkkotallennuspalveluita, Evernoten kaltaisia muistiinpanopalveluita sekä esimerkiksi pilveen tallennettavien salasanojen hallintapalveluita (esim. Lastpass). Tämä kaikki on mahdollista ilman tietoa datan oikeasta sijainnista ja siitä, kuka sitä pääsee käsittelemään. Tietohallinnolla ei välttämättä ole tällaisessa toimintaympäristössä enää varmaa tietoa siitä, missä kaikkialla organisaation data sijaitsee.

Viimeaikaiset paljastukset NSA:n suorittamasta laaja-alaisesta urkinnasta ja useat erilaiset verkon toimintaa uhkaavat haavoittuvuudet (SSLv3 Poodle[33], Heartbleed[34]) eivät ole varsinaisesti lisänneet organisaatioiden intoa siirtää toimintaa julkisiin pilvipalveluihin. Kun tähän uutisointiin lisätään se, että kuluttajalaitteet luontaisesti jakavat tietoa mm. sosiaaliseen mediaan ja erilaisiin pilvipalveluihin, niin kauhuskenaariot tietovuodoista ovat tietoturvasta kiinnostuneiden huolenaiheena. Yrityssalaisuudet voivat pahimmillaan

33 https://www.openssl.org/~bodo/ssl-poodle.pdf (31.1.2015)
34 http://heartbleed.com/ (31.1.2015)

vuotaa kuluttajalaitteiden kautta helposti ja huomaamattomasti johonkin pilveen, mistä niitä ei välttämättä saada koskaan takaisin, eikä käyttäjä edes välttämättä tiedä tästä tiedon siirtymisestä. Voisi olettaa, että suuria uutiskynnyksen ylittäviä tietovuotoja voi odotella juuri kuluttajalaitteisiin ja pilvipalveluiden yleistymiseen liittyen.

Keskeisiä pilvipalveluiden ongelmia ovat:

- niiden hallitsemattomuus – käyttäjät ja myös ostavan osapuolen ylläpitäjät saavat vain rajoitetut hallintamahdollisuudet palveluun,
- pilvipalvelut päivittyvät usein ja saavat uusia ominaisuuksia - asiakkailla ei ole mahdollisuutta jarruttaa tätä kehitystä,
- useissa pilvipalveluissa on lukuisia rajapintoja julkiseen verkkoon, jolloin ne ovat myös suuremmalla todennäköisyydellä hyökkäyksen kohteena,
- pilvipalveluista ei saa helposti perusteellista lokitietoa esim. auditointitarkoituksiin – tätä tietoa ei välttämättä saa ulkomaalaiselta pilvipalvelujen tarjoajalta edes viranomaisten kautta, ja
- useat pilvipalveluiden haavoittuvuudet ovat erityisen vaarallisia johtuen niiden julkisesta luonteesta.

Edellä mainitut ongelmat ovat useille pilvipalveluille tyypillisiä. Lisäksi jopa tietoturvaan erikoistuneiden salasanojenhallintapalveluiden, kuten Lastpass, on huomattu olevan haavoittuvia hyökkäyksille. [Li et al., 2014]

Koska pilvipalvelut ovat käyttäjien kannalta kuitenkin erittäin hyödyllisiä, tulisi organisaatioiden vastata niiden tietoturvahaasteisiin siten, että tarjottaisiin organisaation hallinnoima, mutta käyttäjälle myös helppokäyttöinen palvelukokonaisuus – on se sitten omasta konesalista tai hallitusti ulkoa ostettuna palveluna. Vaihtoehtoja markkinoilla on jo useita. Rajoittamalla olemassa olevien pilvipalveluiden käyttöä tietohallinto saa olla koko ajan varpaillaan ja luoda uusia rajoituksia.

Sen sijaan jos organisaatiolla on tarjota hyvä ja helppokäyttöinen tekninen ratkaisu käyttäjien tarpeisiin ja tätä ratkaisua vielä markkinoidaan ja viestitään käyttäjien suuntaan, niin tietoturvaorganisaatio ei menetä yöuniaan. Tällainen ratkaisu voi jopa parantaa tiedon hallittavuutta, kun voidaan luottaa siihen että valtaosa pilveen tapahtuvista tallennustapahtumista tapahtuu organisaation hallinnoimaan palveluun. Tätä samaa lähestymistä

on myös Cisco käyttänyt menestyksekkäästi oman BYOD-ohjelmansa kanssa [Gruman, 2013].

4.3.5 Henkilöstön osaamiseen liittyvät haasteet

Kuluttajistumisen myötä organisaation IT-infrastruktuuri mullistuu, joko hallitusti tai vähemmän hallitusti. Infran mukaan voi tulla mm. ostettuja pilvipalveluita, oman ympäristön ja pilvipalveluiden väliin rakennettuja integraatioita, moninkertainen määrä uusia laitteita ja laitetyyppejä sekä näiden hallintaan ja rekisteröimiseen tarkoitettuja ohjelmistoja.

Tällaisen kompleksisen infrastruktuurin suunnitelmallinen ja hallittu käyttöönottaminen sekä ylläpitäminen vaativat uudenlaista osaamista organisaation tietohallinnolta. Tämä voi vaatia runsaita panostuksia koulutuksiin sekä resurssien kohdentamista uudelleen esimerkiksi perinteisestä suppeasta mobiililaitteen käyttöönottotuesta (normaali lähituki) kokonaisvaltaisen MDM-ratkaisun ylläpitoon.

Sen lisäksi, että koulutustarpeita voi tulla IT-henkilöstölle, niin BYOD-käytännön myötä tulevat uudet tietoturvariskit voivat aiheuttaa tarvetta henkilöstön kouluttamiselle tietoturvariskien varalta. Panostamalla henkilöstön tietoturvakoulutukseen voi joitakin tietoturvariskejä minimoida, koska joka tapauksessa suurin tietoturvariski organisaation tietojärjestelmille on usein loppukäyttäjä itse [Carman, 2015]. Yksinkertaisimpiakin tietoturvan pelisääntöjä, kuten kieltoa tietoteknisten välineiden lainaamisesta muiden käyttöön, tulisi kerrata ajoittain, muuten ne pääsevät unohtumaan [Lennon, 2012].

Työntekijöiden tietotekninen osaaminen on myös olennaista arvioida ennen omien laitteiden käyttöönottoa. Jos organisaatio esimerkiksi määrittelee BYOD-politiikassaan reunaehdoiksi työasemaa valitessa käyttöjärjestelmän (esim. Windows 8.1 Pro) ja TPM-sirun[35] (Bitlocker[36]-levysalausta varten), niin pitäisi olla varmaa, että käyttäjä varmasti ymmärtää vaatimukset ennen rahojen sijoittamista uuteen laitteeseen. Älypuhelinten osalta ohjeistuksen tekeminen on tällä hetkellä hieman helpompaa, koska muuttujia on työasemiin verrattuna huomattavasti vähemmän. Lähinnä näitä ovat valinnat käyttöjärjestelmiin

[35] http://en.wikipedia.org/wiki/Trusted_Platform_Module (31.1.2015)
[36] http://windows.microsoft.com/en-us/windows7/products/features/bitlocker (31.1.2015)

liittyen. Tietoturvakriittisemmässä ympäristössä älypuhelimiin liittyen voi tulla myös tarkempia määrityksiä, jotta organisaation tietoturvakriteerit tulevat täytetyksi.

5 KULUTTAJISTUMISEN ONGELMAT LOPPUKÄYTTÄJILLE

Organisaation kohtaamien ongelmien lisäksi myös loppukäyttäjä voi omien laitteiden käytön myötä ajautua uusien haasteiden eteen, joita ei perinteisessä IT-ympäristössä esiinny. Seuraavissa kohdissa selvitetään tietoturvallisuuden vaikutusta käyttökokemukseen ja omien laitteiden omatoimiseen hallintaan. Lisäksi selvitetään yksityisyyteen ja laitteiden omistajuuteen liittyvää ongelmakenttää, omien laitteiden tuen järjestelyä sekä vapaa- ja työajan sekoittumisen aiheuttamia ongelmia.

5.1 Tietoturvapolitiikan vaikutus käytettävyyteen

Loppukäyttäjien laitteissa pitäisi pystyä erottamaan henkilökohtainen data organisaation datasta sekä suojella organisaation dataa ja huolehtia samalla työntekijän yksityisyyden säilyttämisestä kansallisen lain ja työntekijöiden kanssa tehtyjen sopimusten mukaisesti. Kaikki tämä suojaaminen pitäisi pystyä tekemään käyttäjälle mahdollisimman helpolla tavalla rampauttamatta esimerkiksi tabletin käytettävyyttä.

Koska tietotekniikkaan liittyvät haasteet ovat lähinnä tietohallinnon ongelma, niin tietohallinnolle voi helposti tulla kiusaus koventaa erityisesti mobiililaitteet mahdollisimman tietoturvalliseksi esimerkiksi tiukalla laitteen lukkiutumisajalla ja toistuvilla PIN-koodi- tai salasanakyselyillä. Lisäksi jos organisaatiossa halutaan antaa käyttäjille muitakin mahdollisuuksia hyödyntää mobiililaitteita kuin pelkkä sähköpostin käyttö, niin IT-toiminnot saattavat sallia esimerkiksi VDI-työpöytäratkaisun kautta resursseihin pääsemisen. Tällä tavalla myös toteutusmielessä päästään helpolla, koska tietokonekäytössä olevien sovellusten saaminen toimimaan VDI-ympäristössä on huomattavasti helpompaa kuin tuottamalla tarkoitusta varten toimiva verkkoselaimen päällä toimiva käyttöliittymä tai natiivi mobiililaitteen sovellus. VDI-ratkaisua käytettäessä kuitenkin mobiililaitteen kosketuskäyttöliittymän edut jäävät helposti saavuttamatta.

Tästä kuluttajistumisen hyötyjen ja tietoturvallisuuden yhteensovittamisesta seuraa ongelmia loppukäyttäjille, mikä on omiaan syömään innostusta ja motivaatiota omien laitteiden hyödyntämisestä.

Omien laitteiden käyttöpolitiikkaa laatiessa tulisikin laitestrategia ja siitä johdetut säännöt ja lopulta yksittäiset tietoturva-asetukset määritellä yhteistyössä liiketoimintojen edustajien kanssa, jotta loppukäyttäjän ääni saataisiin myös kuuluviin. Tämä on olennaista, koska loppukäyttäjät suhtautuvat nihkeästi yleensäkin kaikkiin organisaation asettamiin vaatimuksiin [Vijayan, 2014]. Siksi vaatimusten ja turva-asetusten pitää olla tarkoituksenmukaisia, mutta ei yliampuvia. Samalla tehtyjä pelisääntöjä pitää valvoa ja tarvittaessa pakottaa.

Koska organisaation tietoteknisen ympäristön heikon lenkki tietoturvan kannalta on hyvin usein ihminen itse, niin käyttäjän vastuu turvallisuudesta korostuu erityisesti organisaation verkon ulkopuolella liikkuvien laitteiden myötä. Tästä syystä käyttäjiä pitää kouluttaa tietoturva-asioissa säännöllisesti, jotta he ymmärtävät organisaation asettamat säännöt ja teknisten turva-asetusten tarkoitus. Käyttäjät pystytään sitouttamaan organisaation vaatimuksiin tietoturva-asioissa, kun saadaan samalla viestittyä loppukäyttäjille, mitä hyötyjä sääntöjen noudattamisesta saavutetaan.

Tyypillinen tosielämän tilanne, jonka aiheutumiselta voisi välttyä riittävällä koulutuksella ja opastuksella on se, ettei esimerkiksi jätä organisaation koventamaa älypuhelinlaitetta lojumaan perheen pienempien ulottuville. Tällöin lapsi voi naputella hyvin nopeasti PIN-koodin niin monta kertaa väärin, että yhtiön tietoturvakäytännön mukaisesti laite tyhjennetään esimerkiksi 10 virheellisen koodin syöttämisen jälkeen. Tällaiset tilanteet eivät ole työnantajan eivätkä loppukäyttäjän etu, mutta pienellä ohjeistamisella tällaisiltakin riskeiltä voidaan välttyä.

Kouluttamalla käyttäjiä turvallisiin toimintatapoihin, luomalla yhteistyössä riittävät turva-asetukset ja panostamalla erilaisille päätelaitteille sopivien liiketoimintasovellusten käyttämiselle, voidaan liikkuvasta työvoimasta saada merkittävä voimavara ja hyöty kohtuullisilla tietoturvariskeillä. Toimivan tietoturvapolitiikan luomisessa voi auttaa myös tekniset apuvälineet kuten MDM-tuotteet, joilla voidaan saavuttaa sekä turvallisuutta, valvontaa, että uusia mobiililaitteiden hyötyjä korostavia ominaisuuksia.

Vaikka koulutukset ja tekniset keinot voivat auttaa sekä tietoturvallisuuden että käytettävyyden tavoittelussa, olennaisinta kuitenkin tasapainon löytämisessä on vuoropuhelu tietohallinnon ja loppukäyttäjien välillä.

5.2 Järjestelmänvalvojan oikeudet tai niiden puute

Suurissa organisaatioissa, joissa työvälineiden vakiointi ja tietohallinnon prosessit on viety pitkälle, on hyvin yleistä ja perusteltua, että turvallisuuteen vedoten loppukäyttäjiltä otetaan järjestelmänvalvojan oikeudet pois käytössä olevilta työasemilta. Poikkeustapauksissa esimerkiksi IT-tuen henkilöille tällaiset oikeudet kuitenkin annetaan, jotta heidän tehtävänkuvan mukainen työ ei estyisi. Parhaiden käytäntöjen mukaan IT-henkilöstölläkin tulisi olla omalla työasemalla käytössä ainoastaan peruskäyttäjätunnukset ja ainoastaan tarpeen mukaan suoritettaisiin toimenpiteitä henkilölle myönnetyllä järjestelmänvalvojan tunnuksella.

Tietoturvanäkökulmasta on erittäin oleellista, että organisaation laitteilta ja käyttäjiltä poistetaan sellaiset oikeudet, joille ei ole töiden tekemisen kannalta perusteltua tarvetta. Tällä tavalla mm. haittaohjelmatartuntojen riskiä [Avecto, 2013] ja tietoteknisestä osaamattomuudesta aiheutuvia ongelmia voidaan vähentää. Mikäli loppukäyttäjälle jätetään järjestelmänvalvojan oikeudet omaan tietokoneeseen, niin tällöin käyttäjältä pitäisi edellyttää riittävää tietoteknistä osaamista ja sitoutumista yhtiön tietoturvaohjeistuksiin. Myös vastuukysymykset ongelmatapauksissa pitäisi tuoda esille ennen oman laitteen käyttöönottoa.

Järjestelmänvalvojan oikeuksien tarpeellisuuteen liittyy olennaisella tavalla organisaation toimiala. Esimerkiksi ohjelmistokehittäjille voi olla suorastaan suotuisaa antaa riittävät oikeudet asentaa ohjelmia ja tehdä asetusmuutoksia omiin työvälineisiin. Kehittäjätyötä ei pitäisi lamaannuttaa liiallisilla turvaesteillä. Näissäkin tapauksissa kuitenkin pitäisi tietoturvatasosta huolehtia ja edellyttää samoja pelisääntöjä kuin IT-henkilöstöltä – pääkäyttäjän oikeuksia tulisi hyödyntää vain tarpeen mukaan ja normaalisti toimia työasemilla normaalein käyttäjätunnuksin.

Pääkäyttäjän oikeuksien rajaaminen on ollut yleinen suuntaus jo vuosikaudet. Järjestelmänvalvojan oikeuksia ei tulisi käyttää edes kotikoneissa kuin tarpeen vaatiessa. Microsoftin näkemyksen mukaan järjestelmänvalvojan tunnuksilla työskennellessä ei työaseman turvallisuutta voi taata. Myös useat haittaohjelmien torjuntaan erikoistuneet yritykset suosittelevat käyttämään koneilla normaalisti peruskäyttäjätunnuksia, koska pelkkä hait-

taohjelmatietokantoihin ja haittaohjelmien heuristiseen tunnistamiseen perustuva reaktiivinen turvallisuus ei riitä kaikkien haittaohjelmien torjuntaan. [Avecto, 2013; Laiho, 2014]

Sen sijaan kun konetta suojataan proaktiivisesti mm. poistamalla ylimääräiset käyttöoikeudet ja tämän lisäksi hyödynnetään mm. palomuurien ja haittaohjelmien torjuntaohjelmien käyttöä, voidaan saavuttaa riittävä tietoturvataso koneen päivittäiseen käyttöön tietoverkossa. Lisäturvaa voidaan hakea Applockerin kaltaisista sovelluksista, joilla voidaan rajata sallittujen sovellusten listaa tietohallinnon toimesta.

BYOD-näkökulman kannalta asetelma oikeuksien luovuttamisesta oman laitteen haltijalta organisaation IT-toiminnoille ei kuulosta kuitenkaan luontevalta – erityisesti jos näistä laajemmista oikeuksista oman laitteen haltijana joutuu samalla kokonaan luopumaan. Oman laitteen käyttö työvälineenä tarkoittaa usein sitä, että laitetta käytetään työn lisäksi myös henkilökohtaisiin vapaa-ajan aktiviteetteihin. Tällaisessa tapauksessa järjestelmänvalvojan oikeudet ovat tarpeellisia, jotta vapaa-ajalla voisi hoitaa niitä askareita, joita kotona usein hoidetaan – uusien sovellusten ja laitteiden käyttöönottoa ja asetuksien muokkaamista. Tässä asiassa esim. Windows 7 on harppaus eteenpäin Windows XP -aikakaudesta, koska valtaosa päivittäisistä toimista voidaan hoitaa ilman pääkäyttäjän tunnuksia [MacDonald, 2011], mutta edelleen tulee vastaan tilanteita, joissa pääkäyttäjän oikeuksia tarvitaan.

Omia laitteita saattavat käyttää myös muut perheenjäsenet. Tällaiset asiat tulee ottaa huomioon arvioitaessa BYOD-käytäntöjä. Valitettavan usein kotikoneilla käytetään yhtä ja samaa käyttäjätiliä koko perheen kesken. Jos kotikonetta käytetään työntekoon, niin käyttäjäprofiilit pitäisi erotella tarkasti toisistaan ja varmistaa se, että muilta käyttäjätileiltä ei vahingossakaan pystytä asentamaan koneelle ohjelmistoja, jotka vaarantavat järjestelmän turvallisuuden. Lisäksi organisaation data pitäisi pystyä erottelemaan selkeästi ja turvallisesti henkilökohtaisesta tietosisällöstä.

Järjestelmänvalvojan oikeuksien jättäminen loppukäyttäjille on myös organisaation tietoverkon sisäisten uhkien kannalta arveluttavaa. Esimerkiksi Windows-ympäristössä pahimmillaan osaava järjestelmänvalvojan oikeudet omaava loppukäyttäjä voi hyödyntää ympäristön haavoittuvuuksia hyväkseen ja korottaa omia toimialueoikeuksia esim. toimialueen järjestelmänvalvojan tasolle. Tällaisiltakin sisäisiltä ongelmilta voidaan välttyä rajaamalla järjestelmänvalvojan oikeuksia riittävästi. Pelkkä rajaaminen ei kuitenkaan riitä

esim. Windows-käyttöjärjestelmän kannalta, vaan tarvitaan myös tallennusvälineen kryptausta estämään kiertotiet oikeuksien korottamiseksi.

Jos organisaatiossa sallitaan omien laitteiden käyttö (jotka käyttäjä siis itse omistaa), niin tällöin myös riittävien oikeuksien jättäminen käyttäjälle on perusteltua. Koska tietoturvan näkökulmasta tämä ei ole kuitenkaan kestävää, niin teknisesti voidaan hakea sopivaa kultaista keskitietä esimerkiksi Avecton Defend Point -ohjelmistolla (entiseltä nimeltään Priviledge Guard). Tällä ohjelmistotuotteella voi saada mm. seuraavia ominaisuuksia [Avecto, 2013; 2014]:

- järjestelmänvalvojan oikeudet tarpeen mukaan esimerkiksi soittamalla organisaation omaan tukipalveluun ja pyytämällä korotettuja käyttöoikeuksia puhelimitse (onnistuu challenge-response -menetelmällä myös kun laite ei ole verkossa),
- kattavat lokit kaikista tapahtumista jolloin pääkäyttäjäoikeuksia on käytetty, ja
- sovelluskohtaisia oikeuksia esim. prosessitasolla, jolloin käyttäjälle ei tarvitse antaa korotettuja käyttöoikeuksia, vaikka sovellus niitä vaatisi.

5.3 Yksityisyys ja omistajuus

Työntekijöiden, mutta myös tietohallintojen, kannalta omien laitteiden käytön myötä on edessä uusi tilanne organisaation ja henkilökohtaisen tiedon erottamisen osalta. Normaalisti työnantajan laitteella on pidetty työnantajan dataa ja vain marginaalisesti omia henkilökohtaisia tiedostoja. BYOD-aikakaudella tilanne voi kääntyä päälaelleen ja työhön käytettävällä yksityisellä koneella voi olla valtaosa datasta käyttäjän henkilökohtaista kuten valokuvia, videoita ja asiakirjoja.

Konflikti intresseissä organisaation ja loppukäyttäjän välillä voi olla valmis, kun tietohallinnon yhtenä tehtävänä on turvata organisaation dataa tietovuodoilta sekä väärinkäytöiltä ja vastaavasti loppukäyttäjä, mahdollisena laitteen omistajana, haluaa varjella omaa yksityisyyttään ja määräämisvaltaa omaan laitteeseen. Loppukäyttäjällä voi olla lisäksi vahvoja ennakkoluuloja tietohallinnon toivomia asetusmuutoksia ja turvasovellusten asentamisia kohtaan. Käyttäjät voivat helposti esimerkiksi luulla, että tietoturvaohjelmistot paljastavat käyttäjän yksityisasioita tietohallinnolle [Vijayan, 2014].

Ongelmana useissa organisaatioissa on lisäksi se, että edes organisaatioiden IT ei helposti ole tuomassa kovennuksia laitteille, joita organisaatio ei edes omista. Tämä kevyt linja kuitenkin kiristyy viimeistään siinä vaiheessa, kun tarpeeksi monta kertaa tulee vakavia, laiminlyödystä tietoturvasta tai yksityisyysjärjestelyistä johtuvia ongelmia [Miller et al., 2012].

Valittaessa organisaatiolle BYOD-linjauksia on erittäin tarkasti otettava huomioon juuri tämä käyttäjänäkökulma: Jos joku muu hallinnoi käyttäjän laitetta, niin onko se enää käyttäjän oma laite? [Ackerman, 2013]

Tasapaino turva-asetusten asettamisessa ja käyttäjän päätösvallassa pitää löytää ja se usein löydetään hyvällä viestinnällä ja riittävällä avoimuudella. Tietohallinnon tulisi mm. selvittää käyttäjälle, miksi ja mitä turvakeinoja käyttäjien tuomissa omissa laitteissa tulee käyttää ja miten niiden käyttöä seurataan sekä mitä oikeuksia tietohallinnolla on käyttäjän laitteisiin.

Teknisiä ratkaisuita yksityisyydensuojan ja organisaation datavarantojen turvaamiselle on hiljalleen tullut markkinoille. Muun muassa aiemmin mainitut Windows 8.1 -käyttöjärjestelmän Workplace Join ja Work Folders -ominaisuudet auttavat kuluttajalaitteita liittymään organisaation resursseihin, mutta samalla suojaamaan sisältöjä datan salakirjoituksella ja asettamalla rajan kuluttajapuolen ja organisaatiosovellusten välille. Vastaavasti useat MDM-tuotteiden valmistajat pyrkivät tuomaan apua tähän rajanvetoon.

Vastaavanlaista tekniikkaa on tullut myös älypuhelinmarkkinoille, kuten Samsung Knox[37], jossa työhön kuuluva informaatio säilyy omassa suojatussa ympäristössään siten, ettei käyttäjä saa sitä vahingossakaan vietyä kuluttajapuolen sovellusten käsiteltäväksi [Edwards, 2013]. Tämä Samsung Knox -konsepti saikin mm. Suomessa Viestintävirastolta Katakri II -sertifikaatin, jolloin puhelin kelpaa myös Suomen viranomaisten käyttöön (ST IV-tasolle asti) [NCSA, 2014].

Erityisen vaikeaksi huonosti etukäteen kommunikoidut rajanvedot menevät siinä vaiheessa, kun käyttäjän omistama laite pitää esimerkiksi työsuhteen päättymisen yhteydessä

[37] http://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/ (31.1.2015)

tyhjätä organisaation tietosisällöistä. Samoin kiistanaiheita voivat aiheuttaa niinkin yksinkertaiset asiat kuin puhelinnumerot. Jos työntekijä on saanut hallinnoida omaa puhelinliittymää, jota on käyttänyt toistuvasti työasioiden hoitamiseen, niin jääkö puhelinnumero työntekijälle vai saako työnantaja pitää sen?

Koska laitteiden omistajuusasiat ja yksityisyys ovat BYOD-aikakaudella kriittisiä, tulee tällaiset asiat selvittää kansallisten lakien ja asetusten mukaisesti ja sopia loppukäyttäjien kanssa jo etukäteen ennen omien laitteiden käyttöönottoa. Sopimukset ja tehtävät käytännöt kannattaa tarkistuttaa lakiasiantuntijoilla, jotta vältytään molemminpuoliselta harmilta ja epäselvyyksiltä siinä vaiheessa, kun BYOD-käytännöt ovat jo toteutusvaiheessa.

5.4 Omien laitteiden tuen järjestäminen

Yksi isoista kysymyksistä BYOD-ilmiöön liittyen on: Kuka tai mikä taho tukee omia laitteita? Kuuluuko vastuu koneen toimivuudesta ja tietoturvallisuudesta käyttäjälle vai tukeeko organisaation IT-tukitoiminnot omien työkalujen käytössä ja missä laajuudessa?

Joissakin organisaatioissa tavallisesta poikkeavien laitteiden käytöstä aiheutuviin ongelmiin on löydetty lääke käyttäjien keskinäisestä vertaistuesta. Tällaisella vertaistukiratkaisulle esim. Cisco päästi OS X -koneita IT-ympäristöönsä vuonna 2007 [Gruman, 2013]. Vertaistukiratkaisu on kuitenkin riippuvainen mm. organisaation toimialasta, osaamisesta ja kulttuurista. Nuori IT-alalla oleva startup-yritys varmasti voi pärjätä pitkälle pelkän vertaistuen avulla, mutta suuremmassa organisaatiossa, jossa ikäjakauma ja käyttäjien atk-osaaminen vaihtelee suuresti, ei pelkkä vertaistuki auta.

Toiseksi voidaan kysyä, onko vertaistuella järjestetty ratkaisu aidosti tuottavaa, jos käyttäjät joutuvat itse kamppailemaan tietoteknisten ongelmien kanssa sen sijaan, että käyttäisivät aikaansa tuottavan työn tekemiseen ja antaisivat tukeen erikoistuneiden toimijoiden huolehtia ongelmatilanteiden selvittämisestä? Jo pari tuntia hukkunutta työaikaa koneongelmien ratkaisuun voi olla kustannuksiltaan sitä luokkaa, että vakioitu bisnes-maailman ratkaisu tukipalvelulla voisi tulla halvemmaksi.

Toiseksi omien laitteiden tuen osalta selvittämisen arvoista on eri laitemallien huoltotoimenpiteiden käytännöt. Jos organisaatiossa tehdään tuottavaa työtä sekaisin Dellin, Lenovon ja Applen koneilla, niin miten huolto järjestetään tehokkaasti? Jos organisaatiossa

sallitaan täysin vapaat kädet työasemien valintaan, niin tietohallinnon pitäisi edellyttää käyttäjiltä huoltosopimuksien tekemistä laitetta ostaessa, jotta esimerkiksi laiterikon sattuessa konetta ei tarvitse lähettää viikoiksi korjauskeskukseen, vaan että apu saadaan paikan päälle esimerkiksi seuraavana arkipäivänä. Sen lisäksi, että huoltosopimusten pitää olla kunnossa, tietohallinnon pitää myös järjestää jonkinlainen varalaitteiden varasto, jotta rikkoutumistapauksissa käyttäjille saadaan työnantajan koneita tilalle.

Vaikka periaatteessa organisaatio voi lyhytaikaisesti avustaa vertaistuen voimin omien laitteiden käytöstä aiheutuvaa kuormitusta IT-tukitoiminnoille, niin kovin pitkäaikaisena ratkaisuna tätä ei voida pitää. Vertaistuki voi ruokkia mm. varjo-IT:n kehittymistä, jolloin suuressa organisaatiossa voi syntyä siiloutumista ja toisistaan rajusti poikkeavia tapoja hoitaa tietoteknisiä asioita. Tästä seurauksena voi olla mm. uudet riskit organisaation tietoturvalle.

5.5 Vapaa-ajan ja työajan eron hämärtyminen

Kun raja-aidat työn ja vapaa-ajan välillä edelleen hämärtyvät, voi työssä jaksamisesta tulla entistäkin suurempi ongelma. Jo ensimmäisten mobiililaitteiden push-mail-ratkaisuiden myötä on ollut äärimmäisen helppoa siirtyä kotona vapaa-ajalta hetkeksi ajattelemaan työntekoa, kun puhelin on ilmoittanut saapuneesta sähköpostista. Tekninen mahdollisuus työn jatkamiseen kotona voi huomaamatta lisätä käytännön työaikaa, jota koskaan ei kuitenkaan työaikaseurantajärjestelmään raportoida.

Toisaalta tämän päivän liikkuvassa ja viimeiseen asti aikataulutetussa yhteiskunnassa merkittävä osa työvoimasta jopa arvostaa sitä, että työpaikan käytännöt työn ja vapaa-ajan yhteensovittamisesta ovat joustavia.

Wi-Fi-verkkopalveluja tarjoavan iPass-yhtiön teettämän Mobile Workforce -raportin mukaan [Savvas, 2012] monet kyselyyn vastanneista työläisistä tekevät jopa 20 tuntia viikossa ns. ilmaista työtä työnantajalleen. Tämä johtuu omalta osaltaan juuri työpaikkojen BYOD-käytännöistä. Teknologinen linkki yrityksen järjestelmiin säilyy helposti myös vapaa-ajalla. Tutkimukseen osallistuneista mobiilialan työntekijöistä vain 8 % vetää selvän rajan työn ja vapaa-ajan välille. Vastaavasti 92 % tutkimukseen osallistuneista työntekijöistä nauttii työnantajan mahdollistamasta joustavuudesta ja ovat tyytyväisiä asioiden tilaan, vaikka ilmaista työtä tekevätkin. Tutkimuksessa varoitetaankin, että BYOD-

käytännöt voivat tehdä työntekijöistä liiankin sitoutuneita työhönsä. Pahimpana pelkona ovat tietysti terveydelliset ongelmat ja loppuun palaminen.

Usein tämä ongelma ei välttämättä juonna edes työympäristöstä vaan siitä, että vapauden mukana työntekijät ovat myös valmiita venymään normaalia rankempiin työsuorituksiin.

Perinteinen malli, jossa työtä tehdään työpaikan välineillä, työpaikalla ja ennalta määriteltynä ajankohta, mahdollistaa sen, että työt eivät kulkeudu niin helposti kotioloihin. Varomattomalle tietotyöläiselle voi työ imaista mennessään ja työntekijä saattaa venyä palkkaansa nähden tarpeettomiin suorituksiin. Työnantaja toki tällaisesta voi lyhyellä aika välillä kiittää, mutta pidemmällä aikavälillä pitäisi myös huomioida työntekijöiden työssä jaksaminen.

Suomessa työaikalaki ja yritysten tuntikirjaamisjärjestelmät eivät täysin sovellu toimintamalliin, jossa työpaikka ja työaika ovat häilyviä käsitteitä. Tietotyössä päätelaitevapauden myötä tuleva vapaus paikan ja ajan suhteen aiheuttavat sen, että työntekijän ilmoittamiin työskentelyajankohtiin pitäisi työnantajan ja viranomaisten pystyä luottamaan.

Pitkällä aikavälillä työnantajien tulisi olla varuillaan, jotta mahdollinen BYOD-politiikka ei aiheuttaisi liiallista kuormitusta työntekijöissä. Yksinkertaisin tekninen ratkaisu tilannetta helpottamaan voisi olla esimerkiksi se, että oletuksena organisaation sähköpostia synkronoitaisiin automaattisesti älypuhelimeen vain virka-ajalla.

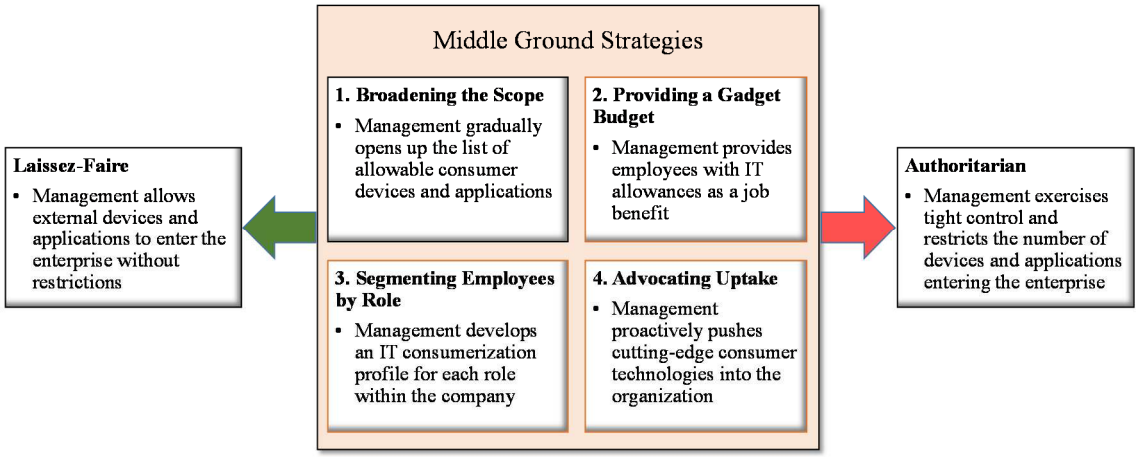
6 TIETOHALLINNON ROOLI MUUTOKSESSA

Tässä luvussa pyritään selvittämään tietohallinnon roolia kuluttajistumiseen liittyvässä muutoksessa. Kohdassa 6.1 pyritään antamaan eväitä siihen, mitä asioita pitäisi BYOD-strategiaa laatiessa muistaa ja kohdassa 6.2 annetaan yksinkertainen esimerkki sellaisesta BYOD-politiikasta, jonka myös loppukäyttäjä voi ymmärtää.

6.1 Ohjeita BYOD-strategian luomiseen

Organisaatioilla tulee olemaan suuria muutoksia edessä kuluttajistumisen seurauksena. Vaikutukset tulevat näkymään niin johdossa, henkilöstöhallinnossa ja tietohallinnossa puhumattakaan siitä vaikutuksesta, miten omien laitteiden, lisääntyvän valinnanvapauden ja sen myötä seuraavan erityisen vastuun seurauksena tapa tehdä tietojenkäsittelyä sivuavaa työtä tulee muuttumaan.

Harrisin ja muiden [2012] mukaan organisaatioiden tavassa johtaa omien laitteiden käyttämistä työn tekemiseen on havaittu kolme päätasoa (ks. kuva 7).



Kuva 7. Kuluttajistumisen johtamisstrategioita. [Harris et al., 2012]

Heidän mukaansa

1) Kolmannes organisaatioista sallii käytännössä kaikkien kuluttajalaitteiden hyödyntämisen työpaikalla. Työntekijät pääosin myös arvostavat tällaista vapautta.
2) Kolmannes organisaatioista rajoittaa kuluttajateknologian käyttämistä työpaikalla tai ainakin pitää ohjat tarkasti omissa käsissään. Näissä turvallisuusnäkökulmat, kustannusten minimointi tiukan vakioinnin myötä ja ylläpidon helpottaminen ovat keskiössä. Tällaista strategiaa voi ajatella hyödynnettävän tietoturvaorientoituneissa ympäristöissä kuten viranomaistoiminnassa ja finanssialalla, joissa toimintaa sitovat joustamattomat lait ja asetukset. Tällaisissa ympäristöissä voisi kuitenkin työntekijöille antaa ainakin näennäisesti valtaa CYOD-käytännöillä – antamalla työntekijöille vakioituja tuotteita, joista voi valita.
3) Kolmannes organisaatioista on keskitien kulkijoita äärimmäisen vapauden ja tiukan kontrollin välimaastossa. Näissä on vielä erotettavissa erilaisia strategioita, joista voi olla käytössä useampi yhtä aikaa:
    a. ”Broadening the Scope”: määritellään hyväksytyt sovellukset ja laitteet sekä politiikat näiden käyttöä varten. Tämä on usein ensimmäinen askel kuluttajistumiseen organisaation sisällä. Haittapuolena on strategian ylläpito, koska tietohallinto on jatkuvasti tutustumassa uuteen tekniikkaan, sovelluksiin ja päivittämässä sääntöjä.
    b. ”Providing Gadget Budget”: tällainen tapa on käytössä mm. Avanadella. Siinä saa työsuhde-etuna vuosittaisen rahasumman, jonka voi sijoittaa haluamallaan tavalla – mutta usein lista hyväksytyistä tekniikoista on rajattu. Tämä on usein käytössä työpaikoissa, joissa on kova teknologinen osaaminen työntekijöillä omasta takaa ja joissa tätä osaamista halutaan ylläpitää. Ongelmia voi tulla kuitenkin monikansallisissa yrityksissä eri maiden verotuskäytännöistä.
    c. ”Segmenting Employees by Role”: työtehtävien mukaan mahdollistetaan tiettyjen laitteiden hyödyntäminen, jos siitä koetaan olevan hyötyä työtehtävien hoitamiseen. Esimerkkinä tästä voisi ajatella tablettien hyödyntämisen liikkuvassa myyntityössä.

d. ”Advocating Uptake”: IT:n johdolla suorastaan kannustetaan uusien laitteiden hyödyntämiseen esimerkiksi hankkimalla uutta teknologiaa varhaisille omaksujille, koska nähdään että uusi tekniikka voi saada aikaan mullistuksia työnteossa tai kilpailukykyä uusien innovaatioiden myötä.

Tutkimus on tehty vuonna 2012 ja mm. Gartnerin arvioiden mukaan [Willis, 2013] vuonna 2015 ympäristö on jo huomattavasti vastaanottavampi kuluttajistumiselle.

Harrisin ja muiden [2012] olennaiset havainnot olivat:

1) Kuluttajistuminen tulee monilla tavoin – puhelimien, tablettien, tietokoneiden ja verkkopalveluiden kautta. Verkon rajoja on hankala jatkossa piirtää ja perinteinen palomuurilla rajattu ympäristö ei enää kuluttajistumisilmiön myötä ole ainoa raja, jota tulisi tietohallinnossa tarkastella.
2) Riittävä turvallisuus on mahdollista saavuttaa. Tutkimuksen näkemyksen mukaan enemmän turvallisuutta pyritään luomaan sovelluksiin ja vähemmän painoarvoa verkon ja itse laitteen suojaukselle. Mobiililaitteissa ja myös tietokoneissa alkaa yleistymään tietosisältöjen lokerointi organisaation datalle. Teknisien keinojen lisäksi olennaista riskien minimoimisessa on käyttäjien kouluttaminen turvallisiin toimintatapoihin [Carman, 2015].
3) Eri maissa on erilaiset säännöt ja lait. USA:n lainsäädäntö on keskimäärin BYOD-käytäntöjä suosivampaa. Siellä myös hyväksytään lainsäädännöllisesti se, että esim. työnantajan sähköposti on työnantajan. Euroopassa tämä on juuri päinvastoin – yksityisyys on kriittistä. Monikansallisten organisaatioiden tulee huomioida kansallisten lakien eroavaisuudet suunnitellessa omien laitteiden käyttöpolitiikkaa.
4) Työvoiman motivaatiot muuttuvat. Nuoret eivät ole enää lojaaleita työnantajiaan kohtaan ja voivat vaihtaa työnantajaa huomattavasti vanhempaa ikäluokkaa rivakammin. Nuoret myös elävät sosiaalisen median keskellä ja haluavat kehittään itseään omilla ehdoillaan. Tällaiseen työvoimaan liian tiukat säännöt ja ohjeistukset eivät toimi.

Edellä mainittujen havaintojen pohjalta mm. Gartnerin listaamat tyypilliset tavoitteet voivat auttaa tekemään BYOD-strategiaa ja johtamaan tästä organisaatiossa käytettäviä pelisääntöjä [Willis, 2013]:

1) organisaation henkilöstön ja mahdollisesti myös yhteistyökumppanien tyytyväisyyden kasvu,
2) mobiliteetin kasvattaminen,
3) ei niin tärkeiden laitteiden hallinnointikuorman siirtäminen pois tietohallinnolta esimerkiksi käyttäjän vastuulle tai vertaistuen pariin,
4) säästöjen saavuttaminen, ja
5) uuden teknologian käyttöönotto kuluttajamarkkinoiden tahdissa ja tästä mahdolliset kilpailuedut innovaatiokyvyn ja organisaation tehokkuuden kasvaessa.

Kun strategiset tavoitteet ovat selvillä, voidaan yhdessä lakiosaston, henkilöstöhallinnon, liiketoimintojen johtajien ja usein myös työntekijöiden edustajien kanssa laatia sopimukset omien laitteiden käytöstä laadittua strategiaa heijastamaan. Sopimuksista pitäisi selvitä mm.

1) kenelle BYOD-oikeudet kuuluvat?
2) kuka korvaa hankintakulut ja mihin rajaan asti?
3) kuka omistaa laitteet?
4) mitä tuetaan ja missä laajuudessa tietohallinnon taholta?
5) mitkä ovat käyttäjien oikeudet ja velvollisuudet?
6) mitä käyttäjä saa tehdä ja mitä ei saa tehdä?
7) miten käyttäjien koulutus tietoturva-asioihin järjestetään?
8) miten huolehditaan käyttäjien yksityisyydestä ja miten tietohallinto voi uutta ympäristöä valvoa?
9) miten menetellään jos sovittuja käytäntöjä rikotaan?

Tällaisien sopimusten laadintaan mm. Gartner tarjoaa sopimusrunkoja[38], joita seuraamalla sopimusten laatiminen voi helpottua.

Koska tekniikka kehittyy kiihtyvään vauhtiin ja organisaatioiden tietojärjestelmät mullistuvat kuluttajistumisen myötä merkittävästi, tulee organisaatioiden kuluttajistumista seuraavien tahojen olla kehityksen kulussa mukana ja kehittää strategiaa ja uudistua sen mukana sekä pitää em. sopimusrungot ajan tasalla.

[38] http://sfcoit.org/modules/showdocument.aspx?documentid=1874 (31.1.2015)

Kuluttajistumisesta saatavat hyödyt voivat olla joillekin organisaatioille kiistattomia. Täydellistä turvallisuutta ei äärimmilleen verkottuneessa BYOD-ympäristössä voi millään saavuttaa. Riskejä voi kuitenkin vähentää ja hyväksyä ilmiön hyötyjen vastapainona tietty määrä riskejä. Infosec-instituutti tiivistää turvallisuus näkökulman hyvin: automatisoi, viesti, opasta, varaudu ongelmiin ja tee toipumissuunnitelma katastrofin varalle [Fox, 2012].

Sen lisäksi, että organisaatiolle on tärkeää laatia strategia ja sopimukset kuluttajistumista tukeviksi (tai rajaaviksi), niin päätetyn BYOD-politiikan vaikutuksia henkilöstön työtyytyväisyyteen tulisi seurata esimerkiksi vuosittain toteutetuilla kyselytutkimuksilla. Näistä voi olla merkittävää hyötyä valitun linjan hyötyjen arvioinnissa.

6.2 Esimerkki omien laitteiden käyttöpolitiikasta

Tässä kohdassa kuvataan esimerkki yksinkertaisesta BYOD-politiikasta, joka toisaalta vapauttaa loppukäyttäjän tekemään joitakin valintoja itse, mutta joka kuitenkin säilyttää työasemiin liittyvän vakioinnin tietohallinnolla itsellään. Tällaisessa BYOD/CYOD-hybridipolitiikassa voisi olla seuraavat ydinkohdat:

Työasema

- Työasema on organisaation omistama, tilaama, hallinnoima, asentama, vakioima ja ylläpitämä.
- Käyttäjä saa valita vapaasti viidestä erilaisesta tuetusta työasemamallista. Esimiehen luvalla poikkeuksia sallitaan, mutta ainoastaan saman laitevalmistajan malleista sekä perustellusta syystä.
- Käyttäjällä ei ole järjestelmänvalvojan oikeuksia työasemaansa. Sovellukset saa valita hyväksyttyjen sovellusten listalta ja uusia sovellustoiveita voi esittää ohjelmistokatselmointi-prosessille. Sovellukset ja päivitykset asennetaan työasemiin keskitetysti.
- Mitään muita laitteita ei saa laittaa työnantajan tietoverkkoon.
- Työsuhteen päättyessä työasemalla oleva työtehtäviin liittyvä materiaali siirretään talteen verkkolevylle ja työaseman levy tyhjennetään turvallisesti ja työasema palautuu tietohallinnolle.

Älypuhelin

- Älypuhelimeksi voi saada organisaation vakiopuhelinmallin tai yhtiö voi rahoittaa matkapuhelinta 250 eurolla. Ylimenevä osa vähennetään seuraavan kuun palkasta. Jos älypuhelin maksaa alle 250 euroa, ei alijäämäosuutta hyvitetä.
- Älypuhelin uusitaan normaalikierron mukaan kerran kahdessa vuodessa.
- Älypuhelimeen voi halutessaan asettaa organisaation postiasetukset erillisen ohjeen mukaisesti, mutta tällöin täytyy hyväksyä laitteeseen tulevat tietoturva-asetukset sekä noudattaa tiettyjä turvaohjeita laitteen käsittelyssä (suojakoodi, laitteen salaaminen).
- Laitteen kadotessa tulee viipymättä ilmoittaa tietohallinnolle, jotta laitteen saa tarvittaessa etänä lukkoon ja/tai etätyhjennettyä.
- Työsuhteen päättyessä älypuhelin palautetaan tehdasasetuksiin ja tämän jälkeen älypuhelimen saa halutessa lunastaa sen jäännösarvolla itselleen.
- Tietohallinnolla on oikeus tyhjentää etänä puhelin mm. puhelimen katoamis- tai varkaustapauksissa tai kun henkilön työsuhde päättyy.
- Älypuhelin on mahdollista liittää toimipisteillä sille erikseen tarkoitettuun langattomaan verkkoon.

Tällaisen kevyen CYOD- ja BYOD-käytäntöjä yhdistävän ohjeistuksen avulla tietohallinto pääsee vähällä ja säilyttää vakioinnin tuomat edut. Samalla kuitenkin loppukäyttäjälle annetaan huomattava valinnanvara älypuhelimen valinnassa ja työasemavalinnassa loppukäyttäjä saa tuetun ja vakioidun tuotteen, mutta saa silti vaikuttaa työaseman malliin omien mieltymyksien ja tarpeiden perusteella.

Malli ei myöskään edellytä hintavien MDM tai muiden hallintaratkaisuiden hankkimista, vaan se on mahdollista saada aikaan hyvin pienillä investoinneilla. Kuitenkaan käyttöpolitiikkaa ei rajaa teknisten ratkaisujen käyttöä ja se mahdollistaa esimerkiksi MDM-tuotteen käyttöönoton vahvistamaan ActiveSync-politiikoilla luotua turvallisuutta sekä tuomaan uusia mahdollisia käyttökohteita mobiililaitteille.

7 YHTEENVETO

Kuluttajistuminen on ilmiö jota juuri mikään organisaatio ei voi sivuuttaa. Ilmiö on hiljalleen vallannut alaa aina IBM PC:n julkistamisesta lähtien, mutta vasta älypuhelimien, tablettien ja langattomien verkkojen kehittyessä nykytilaansa on organisaatioiden tietohallinnon arki alkanut peruuttamattomalla tavalla muuttumaan.

Organisaatioiden on kehitettävä oma BYOD-strategia. Strategiaa voi olla myös se, että sitä ei ole ja antaa ilmiön vain tulla. Tällöin kuitenkin muutoksen johtamisen voi unohtaa. Organisaatioiden tulee ottaa kuluttajistumisilmiö haltuunsa proaktiivisesti ja johtaa muutosta mahdollisuuksien mukaan ja haluamaansa suuntaan. Joka tapauksessa organisaatio päätyy lopulta sallimaan käyttäjille vapauksia, joita ei perinteisesti ole organisaatiossa välttämättä sallittu.

Jos kuluttajistumisen antaa tulla omalla painollaan, niin siitä seuraa helposti varjo-IT:n haittavaikutuksia ja ympäristön kokonaisvaltaista hallitsemattomuutta. Tällaisessa tilanteessa voidaan Bring Your Own Device -ilmiön sijaan puhua Bring Your Own Disaster -tilanteesta. Lisäksi liialliset kiellot ja estot työntekijöiden oma-aloitteiselle työnteon tehokkuuden parantamiselle aiheuttavat helposti tyytymättömyyttä työntekijöissä, jotka saattavat pahimmassa tapauksessa etsiä vapauksia tuovaa työympäristöä muualta.

Tasapainon löytäminen tietoturvallisuuden, käytettävyyden ja yksityisyyden välillä on keskeinen ongelma ilmiön hyötyjen valjastamisessa. Tämän lisäksi pitkään pystyssä olleiden organisaatioiden vanhat tietojärjestelmät ja niiden sovittaminen tähän kosketusnäyttöjen ja erilaisten mobiililaitteiden aikaan voivat tuottaa merkittäviä haasteita ja investointitarpeita.

BYOD-kelkkaan hyppääminen on uusille start up -yrityksille tänä päivänä huomattavan helppoa, koska olemassa olevan infrastruktuurin integroiminen BYOD-maailmaan ei ole aloittelevan yrityksen ongelma. Sen sijaan suurille ja pitkään toimineille organisaatioille BYOD voi aiheuttaa merkittäviä lisäkuluja infrastruktuurin saamiseksi sille tasolle, että kuluttajistumisesta saadaan hyödyt irti ja uhkakuvat torjuttua.

Kuluttajistumista voi organisaation kannalta lähestyä erilaisilla strategioilla ja jokaiselle toimialalle ja kulttuurille löytyy varmasti omansa. Aloittaa voi pienin askelin, esimerkiksi

antamalla valinnanvaraa tietohallinnon vakioitujen laitteiden valintaan. Ensimmäisiä kuluttajistumiselle vapautuvia alueita tulee eteen mobiililaitepuolella – mobiililaitteita kun ei tarvitse välttämättä kytkeä kiinteäksi osaksi organisaation verkkoa, vaan yleensä esimerkiksi sähköpostiratkaisuilla pystytään organisaation viestintämahdollisuuksia käyttämään ilman suoraa kytköstä organisaation sisäverkkoon.

Teknisiä ratkaisuita BYOD-ilmiön haittavaikutusten ja erityisesti tietoturvariskien vähentämiselle on jo runsaasti. Kattavimmat ratkaisut esimerkiksi mobiililaitteiden hallintasovellusten osalta ovat usein kalliita ja vaativia ottaa käyttöön, mutta hyvin monessa tilanteessa ne voivat myös tuoda merkittävää lisäarvoa olemassa oleville laitteiden käyttötavoille sekä rahanarvoisen tietoturvaa parantavan lisän.

IT-maailman kuluttajistuminen on maailmalla levinnyt sellaista vauhtia, että tutkimustietoakin sen vaikutuksia alkaa olemaan ja mm. Gartner tarjoaa yrityksille erilaisia ohjenuoria ilmiön vastaanottamiselle.

Teknisiä ratkaisuita omien laitteiden hallintaa ja tukemista varten on myös. Lukuisia parhaat käytännöt -ohjenuoria kuluttajistumisen vastaanottamiseen löytyy. BYOD-mallin kehittämiselle organisaation tarpeisiin onkin enemmän kyse vain organisaation ja erityisesti tietohallinnon muutosvastarinnasta, nykyajalle tyypillisestä resurssipulasta sekä peloista ja epätietoisuudesta uutta toimintatapaa kohtaan.

VIITELUETTELO

[Accenture, 2010] Accenture, Jumping the boundaries of corporate IT. Accenture global research on Millennials' use of technology, http://nstore.accenture.com/technology/millennials/global_millennial_generation_research.pdf (24.3.2014).

[Ackerman, 2013] Ackerman E., The Bring Your Own Device Dilemma, *IEEE Spectrum*, August 2013, 22.

[Acohido, 2013] Acohido Byron, Using personal devices at work gets more secure, *USA Today*, January 8th 2013, 01b.

[AirWatch, 2012] Airwatch, Enabling Bring Your Own Device (BYOD) In the Enterprise, October 2012, http://www.air-watch.com/solutions/bring-your-own-device-byod (28.3.2014).

[Anderson, 2014] Anderson Neil, Cisco Bring Your Own Device - Device Freedom Without Compromising the IT Network, August 2013, http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.html (9.5.2014).

[Avecto, 2013] Avecto, Microsoft Vulnerabilites Study: Mitigating Risk by Removing User Privileges, 2014, http://learn.avecto.com/2013-microsoft-vulnerabilities-report-d (28.3.2014).

[Avecto, 2014] Avecto, PwC Switzerland Case Study, October 23rd 2014, http://www.avecto.com/resources/case-studies/pwc-switzerland-case-study/ (11.11.2014).

[Arthur and Fox, 2011] Arthur Charles and Fox Killian, How the iPad revolution has transformed working lives, *The Observer*, March 27th 2011, http://www.theguardian.com/technology/2011/mar/27/ipad-tablet-computer-users-rivals (23.6.2014).

[Carman, 2015] Carman Ashley, Investment in end-user training could reduce cost by 60 percent, *SC Magazine*, January 15th 2015, http://www.scmagazine.com/risk-model-shows-investment-in-user-training-lowers-company-cost/article/392612/ (20.1.2015).

[Carr, 2013] Carr David F., Tablets To Edge PCs In Q4: IDC, *Information Week*, September 12th 2013, http://www.informationweek.com/desktop/tablets-to-edge-pcs-in-q4-idc/d/d-id/1111515 (28.3.2014).

[Dahlstrom, 2013] Dahlstrom Eden, Executive Summary: BYOD and Consumerization of IT in Higher Education Research, *EDUCAUSE Review*, April 1st 2013, http://www.educause.edu/ero/article/executive-summary-byod-and-consumerization-it-higher-education-research-2013

[Dahlstrom and diFilipo, 2013] Dahlstrom Eden and diFilipo Stephen, The Consumerization of Technology and the Bring-Your-Own-Everything (BYOE) Era of Higher Education, March 25th 2013, 1-43, http://net.educause.edu/ir/library/pdf/ERS1301/ERS1301.pdf (1.4.2014)

[Edwards, 2013] Edwards Chris, Identity – the new security perimeter, *Computer Fraud & Security*, 2013, 9, September 2013, 18-19.

[Foley, 2014] Foley Mary Jo, Microsoft to make per-user Windows licensing available to enterprise customers, November 2014, http://www.zdnet.com/article/microsoft-to-make-per-user-windows-licensing-available-to-enterprise-customers/ (5.11.2014).

[Fox, 2012] Fox John, Top 10 Tips for Securely Managing Your Employee's BYOD, Infosec Institute, February 3rd 2012, http://resources.infosecinstitute.com/tips-managing-byod-security/ (5.11.2014).

[Fujitsu, 2012] Fujitsu Finland Oy, Fujitsun uusi Patja Easy tuo kehittyneen työympäristön kotikoneeseen, Fujitsu Finland Oy – tiedotearkisto, http://www.fujitsu.com/fi/about/resources/news/press-releases/2012/patja_easy.html (9.5.2014).

[Gartner, 2014] Gartner, Press Release: Gartner Says Worldwide PC Shipments Declined 6.9 Percent in Fourth Quarter of 2013, January 2014, http://www.gartner.com/newsroom/id/2647517 (28.3.2014).

[Gartner, 2012] Gartner, Press Release: Gartner Says Cloud, Mobility and Open Source Will Drive Application Development Market to Exceed $9 Billion in 2012, August 2012, http://www.gartner.com/newsroom/id/2131115 (22.5.2014).

[Greengard, 2012] Greengard Samuel, How Steve Jobs Revolutionized Business, *ACM News*, May 2012, http://cacm.acm.org/opinion/articles/149292-how-steve-jobs-revolutionized-business/fulltext# (24.3.2014).

[Gruman, 2013] Gruman, Galen, Cisco shows how to manage 35,000 Macs, September 2013, http://www.infoworld.com/d/consumerization-of-it/cisco-shows-how-manage-35000-macs-226305?source=fssr (28.3.2014).

[Harris et al., 2012] Harris Jeanne, Ives Blake, Junglas Iris, IT Consumerization: When Gadgets Turn Into Enterprise IT Tools, *MIS Quarterly Executive*, September 2012, p. 99-112. https://informationstrategyrsm.files.wordpress.com/2012/09/it-consumerization-when-gadgets-turn-into-enterprise-it-tools.pdf (10.11.2014).

[Hester, 2013] Hester Matt, Why Windows Server 2012 R2: Step-by-Step Workplace Join, Bringing Peace of Mind for BYOD, TechNet Blogs, November 2013, http://blogs.technet.com/b/matthewms/archive/2013/11/01/why-windows-server-2012-r2-step-by-step-workplace-join-bringing-peace-of-mind-for-byod.aspx (14.1.2015).

[IBM, 2010] IBM Lotus Domino and Notes Information Center, IBM Lotus Notes Traveler 8.5.1 Overview, http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/topic/com.ibm.help.lnt851.doc/LNT_overview.html (2.5.2014).

[Jeffrey, 2011] Jeffrey Burt, BYOD Trend Pressures Corporate Networks, *eWeek*, September 5th 2011, 30-31.

[Kantar, 2014] Kantar Worldpanel ComTech, *Press Information*, Apple regains momentum as Windows stutters, http://www.kantarworldpanel.com/global/News/Apple-regains-momentum-as-Windows-stutters (16.6.2014).

[Kasvi, 2014] Kasvi Jyrki J.J., Teknologian murros vaatii ketterää sääntelyä, *Eurooppa 2.0 Eurooppa digitaalisen murroksen kourissa*, huhtikuu 2014, 30 http://www.eurooppapaiva.fi/assets/publications/01-36eurooppalainensuomi_netti.pdf (11.4.2014).

[Katakri2, 2011] KATAKRI, Kansallinen turvallisuusauditointikriteeristö, 2011, http://www.defmin.fi/hallinnonala/puolustushallinnon_turvallisuustoiminta/kansallinen_turvallisuusauditointikriteeristo_(katakri) (9.10.2014).

[Lacey, 2013] Lacey Kylie, Consumer Technologies Enter Schools, *District Administration*, 49, 5, May 2013, 58-61.

[Laiho, 2014] Laiho Sami, Proactive Security Beats Reactive Security, *Win-Fu Blog*, August 29th 2014, http://blog.win-fu.com/2014/08/proactive-security-beats-reactive.html (10.9.2014).

[Lennon, 2012] Lennon R.G., Changing User Attitudes to Security in Bring Your Own Device (BYOD) & the Cloud, *Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania*, October 2012, 49-52.

[Li et al., 2014] Li Zhiwei, He Warren, Akhawe Devdatta and Song Dawn, The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, http://devd.me/papers/pwdmgr-usenix14.pdf (15.7.2014).

[MacDonald, 2011] MacDonald Neil, Removing Administrator Rights for Windows Users is not "Lockdown", Gartner, May 4th 2011, Removing Administrator Rights for Windows Users is not "Lockdown" (10.7.2014).

[McIlwain, 2011] McIlwain Matt, BYOA: The New Path Into The Enterprise For Savvy Startups, Forbes, August 3rd 2011, http://www.forbes.com/sites/ciocentral/2011/08/03/byoa-the-new-path-into-the-enterprise-for-savvy-startups/ (14.12.2014).

[Mell and Grance, 2011] Mell Peter and Grance Timothy, The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, *NIST Special Publication 800-145*, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (22.5.2014).

[Mello, 2013] Mello John, ActiveSync isn't just for Exchange anymore, October 2012, http://www.theemailadmin.com/2012/10/activesync-isnt-just-for-exchange-anymore/ (24.3.2014).

[Microsoft, 2013] Microsoft Security Intelligence Report, 15, June 2013.

[Microsoft, 2014a] Microsoft Legal and Corporate Affairs, Exchange ActiveSync Protocol, http://www.microsoft.com/en-us/legal/intellectualproperty/IPLicensing/Programs/exchangeactivesyncprotocol.aspx (24.3.2014).

[Microsoft, 2014b] Microsoft, What's new in Windows 8.1, http://technet.microsoft.com/en-us/windows/dn140266.aspx (7.1.2015).

[Microsoft, 2014c] Microsoft, Bring Your Own Device (BYOD) – New Windows Server 2012 R2 Device Access and Information Protection, *Windows Server Blog*, http://blogs.technet.com/b/windowsserver/archive/2013/06/28/bring-your-own-device-byod-new-windows-server-2012-r2-device-access-and-information-protection.aspx

[Miller et al., 2012] Miller Keith W., Voas Jeffrey and Hurlburt George F., BYOD: Security and Privacy Considerations, *IT Professional*, 14, 5, September / October 2012, 53-55.

[Miradore, 2015] Miradore, Features by platform – Miradore Online Support, http://onlinesupport.miradore.com/hc/en-us/articles/200691872 (28.1.2015).

[Moody, 2013] Moody Joseph, Workplace Join overview, *4Sysops*, https://4sysops.com/archives/workplace-join-overview/ (21.11.2014).

[Moschella et al., 2004] Moschella David, Neal Doug, Opperman Piet and Taylor John, The 'Consumerization' of Information Technology Position Paper, 2004, http://www.lef.csc.com/publications/281 (28.3.2014).

[NCSA, 2014] Kyberturvallisuuskeskus suojaa luokiteltua tietoa, Viestintävirasto, Kyberturvallisuuskeskus, https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/09/ttn201409301451.html (5.10.2014).

[Oltsik, 2014] Oltsik Jon, Why VMware bought AirWatch, Network World, January 2014, http://www.networkworld.com/community/blog/why-vmware-bought-airwatch (28.3.2014).

[O'Reilly, 2005] O'Reilly Tim, What Is Web 2.0, http://www.oreilly.com/lpt/a/1 (20.1.2015).

[Pervilä, 2013] Pervilä Markku, Oma laite voi viedä yrityksen raastupaan, Tietoviikko, 24.4.2013, http://www.tietoviikko.fi/cio/oma+laite+voi+vieda+yrityksen+raastupaan/a896923 (28.3.2014).

[Peters, 2008] Peters Chris, Tips for Standardizing Your IT Infrastructure, TechSoup, July 7th 2008, https://www.techsoup.se/node/810 (10.11.2014).

[Rangaswami, 2012] Rangaswami, M.R., Hidden Cost Factors and Total Cost of Ownership for Enterprise Mobility, April 2012, http://sandhill.com/article/hidden-cost-factors-and-total-cost-of-ownership-for-enterprise-mobility/ (28.3.2014).

[Redman et al., 2013] Redman Philip, Girard John, Cosgrove Terrence and Basso Monica, Magic Quadrant for Mobile Device Management Software, Gartner, May 23rd 2013.

[Remde, 2013] Remde Kevin, What's New for Active Directory in Server 2012 R2, TechNet Blogs, http://blogs.technet.com/b/kevinremde/archive/2013/10/30/what-s-new-for-active-directory-in-server-2012-r2.aspx (14.1.2015).

[Sangani, 2013] Sangani Kris, BYOD to the classroom, *Engineering & Technology*, 8, 3, April 2013, 42-45.

[Savvas, 2012] Savvas Anthony, BYOD makes employees work extra 20 hours unpaid, *Computerworld UK*, August 2012, http://www.cio.co.uk/news/budgeting/byod-makes-employees-work-extra-20-hours-unpaid/ (2.5.2014).

[Scarfò, 2012] Scarfò Antonio, New Security Perspectives around BYOD, *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, November 2012, 446-451.

[Smith, 2012] Smith Russell, Using DHCP Policy-Based Assignment in Windows Server 2012, Petri IT Knowledgebase, http://www.petri.co.il/dhcp-policy-based-assignment-windows-server-2012.htm (14.1.2015).

[Talouselämä, 2013] Nokia ulkoisti Intiassa - uusi työnantaja ei anna työntekijöilleen edes matkapuhelimia, Talouselämä, 20.2.2013, http://www.talouselama.fi/uutiset/nokia+ulkoisti+intiassa++uusi+tyonantaja+ei+anna+tyontekijoille+edes+matkapuhelimia/a2170402 (28.3.2014).

[Vijayan, 2014] Vijayan Jaikumar, There's Still a Security Disconnect on BYOD, *Computerworld*, July 11th 2014, http://www.cio.com/article/2452692/byod/theres-still-a-security-disconnect-on-byod.html (15.7.2014).

[Wakefield Research, 2012] Wakefield Research, Global Survey: Dispelling Six Myths of Consumerization of IT, January 2012, http://www.avanade.com/Documents/Resources/consumerization-of-it-executive-summary.pdf (28.3.2014).

[Weiss, 2013] Weiss Todd R., Google Adds BYOD Management Tools for Android, *eWeek*, July 1st 2013, 5-5.

[Wikipedia ActiveSync, 2013] Wikipedia-artikkeli: Comparison of Exchange ActiveSync Clients, December 2013, http://en.wikipedia.org/wiki/Comparison_of_Exchange_ActiveSync_clients (24.3.2014)

[Wikipedia, 2013] Wikipedia: Cloud Computing, January 2013. http://en.wikipedia.org/wiki/Cloud_computing#Service_models (28.3.2014).

[Wikipedia, 2014] Wikipedia: Internet, http://fi.wikipedia.org/wiki/Internet (28.3.2014).

[Wikipedia 802.1X, 2014b] Wikipedia: IEEE 802.1X, http://en.wikipedia.org/wiki/IEEE_802.1X (24.1.2015).

[Wikipedia iPad, 2014] Wikipedia: iPad, http://en.wikipedia.org/wiki/IPad (3.6.2014).

[Willis, 2013] Willis, David A., Bring Your Own Device Program Best Practices (BYOD), August 2013.

[Wziatek-Ladosz, 2013] Wziatek-Ladosz Joanna, 10 problems Sophos can solve - A guide for the IT department, *Webinar*, September 10th 2013.

LIITE: KULUTTAJISTUMISEEN LIITTYVÄÄ TERMINOLOGIAA

Kuluttajistumisilmiöön liittyy läheisesti mm. seuraavia englanninkielisiä lyhenteitä / termejä, joita tämä tutkielma sivuuttaa.

Lyhenne / käsite	Selitys
Active Directory	Microsoft Windows-toimialueen keskeinen komponentti - hakemistopalvelu, jossa on rekisteröityneenä mm. käyttäjät, koneet ja muut verkkoresurssit
ADFS (Active Directory Federation Services)	Microsoftin kehittämä palvelu, jolla on mahdollista mm. tuoda organisaation tunnuksiin ja verkkoon pohjautuva kirjautuminen osaksi oman IT-ympäristön ulkopuolella olevia palveluita. Federointiratkaisuja ja standardeja on lukuisia, joista ADFS on mainittu esimerkkinä osana tässä tutkielmassa.
BYOA (Bring Your Own Application / Anything)	Termi, joka keskittyy käsitykseen omien sovellusten tuomisesta osaksi organisaation tietoteknistä ympäristöä.
BYOC (Bring Your Own Computer / Cloud)	Harvoin käytetty lyhenne, jolla yleensä tarkoitetaan oman tietokoneen tuomista osaksi organisaation IT-ympäristöä. Joissakin yhteyksissä tällä lyhenteellä tarkoitetaan omien pilvipalveluratkaisujen tuominen osaksi työympäristöä.
BYOD (Bring Your Own Device)	Vakiintunein ja tunnetuin kuluttajistumista sivuava termi, jolla usein käsitetään käytännössä kaiken kuluttajateknologian tuomista työpaikoille – on se sitten tietokoneita, älylaitteita, sovelluksia tai pilviratkaisuita.
BYOE (Bring Your Own Everything)	Yleistermi kuluttajistumiseen liittyen, harvoin käytetty
BYOI / BYOID (Bring Your Own Identity)	Termi, joka keskittyy identiteettiin ja usein kaksoisidentiteettiin - henkilökohtaiseen ja työ-minään. BYOI-termillä yleensä viitataan ratkaisuihin, joissa henkilökohtainen tietosisältö ja organisaation data voidaan erottaa toisistaan teknisesti.
BYOPC (Bring Your Own Personal Computer)	Harvoin käytetty lyhenne eikä erityisen vakiintunut. Tarkoituksena tällä on kuvata omien tietokoneiden hyödyntämistä työssä.
BYOT (Bring Your Own Technology)	Yleistermi, harvoin käytetty. Periaatteessa sisältää useita em. käsitteitä, mutta käytännössä tämän sijaan käytetään usein lyhennettä BYOD.
CoIT (Consumerization of IT)	Yleistermi kuluttajistumiseen liittyen. Ei keskity niinkään laitteisiin ja teknologiaan vaan tapaan, jolla työntekeminen muuttuu.
CYOA (Choose Your Own Applications)	Termi, joka keskittyy käsitykseen omien sovellusvalintojen tuomisesta osaksi organisaation tietoteknistä ympäristöä. Organisaatioissa saatetaan käyttää, jonkinlaista hyväksyntäprosessia (Software Asset Management) hyväksymään tehdyt sovellusvalinnat.

CYOC (Choose Your Own Computer)	Harvoin käytetty termi. Kuvaa mahdollisuuksia valita tietokone IT:n hyväksymältä listalta.
CYOD (Choose Your Own Devices)	BYOD-termin jälkeen toiseksi vakiintunein käsite. Kuvaa samaa asiaa, mutta yleensä tällä tarkoitetaan sitä, että tietohallinto määrittelee listan hyväksyttyjä laitteita, joista käyttäjä saa tehdä valintansa. Näin ollen valinnanvapaus on tarkemmin rajattu.
IRM (Information Rights Management)	Tekniikkaa, jolla luotettavaa tietoa suojataan mm. kryptaamisella ja oikeuksien määrittelyllä siihen, miten ja kuka suojattua informaatiota voi käsitellä.
MAM (Mobile Application Management)	MAM-ratkaisut ovat usein MDM-tuotteisiin sisältyviä. MAM-ratkaisut keskittyvät enemmän sovellusten hallintaan eivätkä varsinaisen laitteen hallintaan kuten MDM-tuotteet.
MDM (Mobile Device Management)	Mobiililaitteiden hallinta järjestelmä, jolla saadaan lukuisat laitteet keskitetyn hallinnan piiriin. Nykyiset MDM-ratkaisut mahdollistavat myös joitakin työasemanhallintaan liittyviä toiminnallisuuksia.
Office 365 / O365	Tutkielmassa mainittu Microsoftin Office 365 -pilvipalvelu, joka sisältää mm. Exchange-sähköpostipalveluita, pikaviestintää (Lync), tiedostopalveluita yms.
PKI	Julkisten avainten hallintajärjestelmä - keskeinen osa varmenteisiin perustuvien salausjärjestelmien käyttöä
VDI (Virtual Desktop Infrastructure)	Järjestelmä, jolla mm. virtuaalinen käyttöjärjestelmä (esim. Windows 7) tuodaan loppukäyttäjän saataville esim. Remote Desktop -protokollan avulla.